



# The FortiGate Cookbook

Recipes for Success with your FortiGate

FortiOS 5.2



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



Fortinet Cookbook - <http://cookbook.fortinet.com>

Fortinet Knowledge Base - <http://kb.fortinet.com>

Technical Documentation - <http://docs.fortinet.com>

Video Tutorials - <http://video.fortinet.com>

Training Services - <http://campus.training.fortinet.com>

Technical Support - <https://support.fortinet.com>

Please report errors or omissions in this or any Fortinet technical document to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

# Table of Contents

- Change Log ..... 8**
- Introduction ..... 9**
- Tips ..... 10**
- Getting Started ..... 12**
  - Choosing your FortiGate's switch mode ..... 14
  - Installing a FortiGate in NAT/Route mode ..... 15
  - Installing a FortiGate in Transparent mode ..... 21
  - Quick installation using DHCP ..... 27
  - Redundant Internet connections ..... 31
  - Troubleshooting your FortiGate installation ..... 36
  - FortiGate registration and basic settings ..... 40
  - Updating your FortiGate's firmware ..... 45
  - Setting up FortiGuard services ..... 49
  - FortiGuard troubleshooting ..... 55
  - Logging FortiGate traffic ..... 56
  - Logging with FortiCloud ..... 60
  - Troubleshooting FortiGate logging ..... 65
  - Creating security policies ..... 66
  - Limited access administrator accounts ..... 72
  - Port pairing in Transparent mode ..... 77
  - How to upgrade one unit in an HA cluster ..... 81
  - Port forwarding ..... 87
  - FortiGuard DDNS ..... 93
  - SNMP monitoring ..... 96
  - Packet capture ..... 103
  - VDOM configuration ..... 107
  - High Availability with two FortiGates ..... 115
  - AirPlay for Apple TV ..... 122

|  |            |
|--|------------|
| Protect a web server with DMZ .....                        | 127        |
| Traffic shaping for VoIP .....                             | 132        |
| Creating an IPv6 interface using SLAAC .....               | 141        |
| FortiExtender installation .....                           | 144        |
| Remotely accessing FortiRecorder through a FortiGate ..... | 150        |
| Managing a FortiSwitch with a FortiGate .....              | 162        |
| <b>Authentication .....</b>                                | <b>164</b> |
| User and device authentication .....                       | 166        |
| Excluding users from security scanning .....               | 174        |
| FSSO in Polling mode .....                                 | 178        |
| Two-factor authentication with FortiToken Mobile .....     | 184        |
| <b>Security .....</b>                                      | <b>191</b> |
| FortiOS AntiVirus inspection modes .....                   | 193        |
| AntiVirus with FortiSandbox .....                          | 195        |
| Blocking Ultrasurf .....                                   | 201        |
| Blocking P2P traffic and YouTube applications .....        | 205        |
| Blocking Windows XP traffic .....                          | 212        |
| Blocking and monitoring Tor traffic .....                  | 217        |
| Controlling access to Apple's App Store .....              | 222        |
| Restricting online gaming to evenings .....                | 227        |
| Preventing data leaks .....                                | 233        |
| Prevent credit card numbers from being leaked .....        | 238        |
| Protecting a web server .....                              | 242        |
| Logging DNS domain lookups .....                           | 247        |
| Why you should use SSL inspection .....                    | 252        |
| Preventing certificate warnings .....                      | 255        |
| Exempting Google from SSL inspection .....                 | 268        |
| Blocking Facebook .....                                    | 273        |
| Blocking adult/mature content with Google SafeSearch ..... | 278        |

|   |            |
|---|------------|
| Web rating overrides .....                                      | 287        |
| Web filtering using quotas .....                                | 292        |
| Blocking Google access for consumer accounts .....              | 297        |
| Overriding a web filter profile .....                           | 300        |
| Troubleshooting web filtering .....                             | 305        |
| <b>VPNs .....</b>   | <b>306</b> |
| IPsec VPN with FortiClient .....                                | 308        |
| IPsec VPN for iOS devices .....                                 | 314        |
| IPsec VPN with the native Mac OS client .....                   | 323        |
| IPsec VPN with two-factor authentication .....                  | 330        |
| IPsec VPN with external DHCP service .....                      | 341        |
| Site-to-site IPsec VPN with two FortiGates .....                | 349        |
| Site-to-site IPsec VPN with overlapping subnets .....           | 355        |
| IPsec VPN to Microsoft Azure .....                              | 362        |
| Remote Internet browsing using a VPN .....                      | 372        |
| Remote browsing using site-to-site IPsec VPN .....              | 379        |
| IPsec troubleshooting .....                                     | 386        |
| SSL VPN for remote users .....                                  | 388        |
| SSL VPN using FortiClient for iOS .....                         | 399        |
| SSL VPN for Windows Phone 8.1 .....                             | 406        |
| SSL VPN with certificate authentication .....                   | 412        |
| SSL VPN with RADIUS authentication .....                        | 423        |
| RADIUS authentication for SSL VPN with FortiAuthenticator ..... | 436        |
| LDAP authentication for SSL VPN with FortiAuthenticator .....   | 442        |
| SSL VPN remote browsing with LDAP authentication .....          | 449        |
| SMS two-factor authentication for SSL VPN .....                 | 455        |
| SSL VPN troubleshooting .....                                   | 462        |
| <b>WiFi .....</b>   | <b>464</b> |
| Setting up WiFi with FortiAP .....                              | 466        |

|   |            |
|---|------------|
| Setting up a WiFi bridge with a FortiAP .....                             | 471        |
| Combining WiFi and wired networks with a software switch .....            | 475        |
| WiFi network with external DHCP service .....                             | 479        |
| Providing remote access to the office and Internet .....                  | 483        |
| Extending WiFi range with mesh topology .....                             | 489        |
| Explicit proxy with web caching .....                                     | 495        |
| Guest WiFi accounts .....   | 502        |
| Captive portal WiFi access control .....                                  | 507        |
| WP2A WiFi access control .....  | 512        |
| MAC access control .....  | 516        |
| BYOD scheduling .....   | 521        |
| BYOD for a user with multiple wireless devices .....                      | 525        |
| WiFi RADIUS authentication with FortiAuthenticator .....                  | 529        |
| Using an external captive portal for WiFi security .....                  | 534        |
| Assigning WiFi users to VLANs dynamically .....                           | 540        |
| WiFi with Wireless Single Sign-on .....                                   | 548        |
| RSSO WiFi access control .....  | 555        |
| Social WiFi Captive Portal with FortiAuthenticator (Facebook) .....       | 566        |
| Social WiFi Captive Portal with FortiAuthenticator (Twitter) .....        | 580        |
| Social WiFi Captive Portal with FortiAuthenticator (Google+) .....        | 589        |
| Social WiFi Captive Portal with FortiAuthenticator (LinkedIn) .....       | 600        |
| Social WiFi Captive Portal with FortiAuthenticator (Form-based) .....     | 612        |
| <b>Expert .....</b>   | <b>619</b> |
| High Availability with FGCP .....   | 620        |
| Redundant architecture .....  | 628        |
| SLBC setup with one FortiController-5103B .....                           | 641        |
| SLBC Active-Passive setup with two FortiController-5103Bs .....           | 646        |
| SLBC Active-Passive with two FortiController-5103Bs and two chassis ..... | 654        |
| SLBC Dual Mode with two FortiController-5103Bs .....                      | 669        |

SLBC Active-Passive with four FortiController-5103Bs and two chassis .....677

SLBC Dual Mode with two FortiController-5903Cs .....696

BGP over a dynamic IPsec VPN .....719

OSPF over dynamic IPsec VPN .....725

Single Sign-on using LDAP and FSSO agent in advanced mode .....732

Single Sign-On using FSSO agent in advanced mode and FortiAuthenticator .....741

SSO using a FortiGate, FortiAuthenticator, and DC Polling .....753

Hub-and-spoke VPN using quick mode selectors .....760

**Glossary .....770**



# Change Log

| Date         | Change description                                |
|--------------|---|
| Nov 20, 2015 | Added and updated recipes throughout.             |
| Oct 2, 2015  | Corrected recipe Preventing certificate warnings. |
| May 12, 2015 | Initial publication                               |

# Introduction

FortiGate is a network security appliance that can apply a number of features to your network traffic, providing a consolidated security solution to match the needs of any network, big or small.

The FortiGate recipes is divided into the following sections:

- **Getting Started:** recipes to help you start using your FortiGate.
- **Authentication:** recipes about authenticating users and devices on your network.
- **Security:** recipes about using a FortiGate to protect your network.
- **VPNs:** recipes about virtual private networks (VPNs), including authentication methods.
- **WiFi:** recipes about managing a wireless network with your FortiGate.
- **Expert:** recipes about advanced FortiGate configurations for users with a higher degree of background knowledge.

This version of the complete FortiGate cookbook was written using FortiOS 5.2.4.

# Tips

Before you get started, here are a few tips about using the FortiGate Cookbook:

## Understanding the basics

Some basic steps, such as logging into your FortiGate, are not included in most recipes. This information can be found in the [QuickStart guide](#) for your product.

## Screenshots vs. text

The FortiGate Cookbook uses both screenshots and text to explain the steps of each example. The screenshots display the entire configuration, while the text highlights key details (i.e. the settings that are strictly necessary for the configuration) and provides additional information. To get the most out of the FortiGate Cookbook, start with the screenshots and then read the text for more details.

## Model and firmware

GUI menus, options, and interface names may vary depending on the which model you are using and the firmware build.

For example, some FortiGate models do not have the menu option **Router > Static > Static Routes**.

## Ports

The specific ports being used in the documentation are chosen as examples. When you are configuring your unit, you can substitute your own ports, provided that they have the same function.

For example, in most recipes, wan1 is the port used to provide the FortiGate with access to the Internet. If your FortiGate uses a different port for this function, you should use that port in the parts of the configuration that the recipe uses wan1.

## IP addresses and object names

IP addresses are sometimes shown in diagrams to make it easier to see the source of the addresses used in the recipe. When you are configuring your product, substitute your own addresses. You should also use your own named for any objects, including user accounts, that are created as part of the recipe. Make names as specific as possible, to make it easier to determine later what the object is used for.

## Text elements

**Bold text** indicates the name of a GUI field or feature. When required, *italic text* indicates information that you must enter.

*Italic text* is also used for notes, which contain information that you may find useful while using a recipe.

## Selecting OK/Apply

Always select **OK** or **Apply** when you complete a GUI step. Because this must be done frequently, it is an assumed step and is not included in most recipes.

## IPv4 vs IPv6 policies

Most recipes in the FortiGate Cookbook use IPv4 security policies. However, the majority of them could also be done using IPv6 policies. If you wish to create an IPv6 policy, go to **Policy & Objects > Policy > IPv6**.

## Turning on FortiOS features

Some FortiOS features can be turned off, which means they will not appear in the GUI. If an option required for a recipe does not appear, go to **System > Config > Features** and make sure that option is turned on.

Also, on some FortiGate models, certain features are only available using the CLI. For more information about this, see the [Feature/Platform Matrix](#).

# Getting Started

This section contains information about basic tasks to get a FortiGate unit up and running, including installation, as well common roles and configurations a FortiGate unit can have in your network.

## Installation

- [Choosing your FortiGate's switch mode](#)
- [Installing a FortiGate in NAT/Route mode](#)
- [Installing a FortiGate in Transparent mode](#)
- [Quick installation using DHCP](#)
- [Redundant Internet connections](#)
- [Troubleshooting your FortiGate installation](#)

## Setting up your FortiGate

- [FortiGate registration and basic settings](#)
- [Updating your FortiGate's firmware](#)
- [Setting up FortiGuard services](#)
- [FortiGuard troubleshooting](#)
- [Logging FortiGate traffic](#)
- [Logging with FortiCloud](#)
- [Troubleshooting FortiGate logging](#)
- [Creating security policies](#)
- [Limited access administrator accounts](#)
- [Port pairing in Transparent mode](#)
- [How to upgrade one unit in an HA cluster](#)

## Common configurations

- [Port forwarding](#)
- [FortiGuard DDNS](#)
- [SNMP monitoring](#)
- [Packet capture](#)
- [VDOM configuration](#)

- High Availability with two FortiGates
- AirPlay for Apple TV
- Protect a web server with DMZ
- Traffic shaping for VoIP
- Creating an IPv6 interface using SLAAC

## Using a FortiGate with other Fortinet products

- FortiExtender installation
- Remotely accessing FortiRecorder through a FortiGate
- Managing a FortiSwitch with a FortiGate



# Choosing your FortiGate's switch mode

This section contains information to help you determine which internal switch mode your FortiGate should use, a decision that should be made before the FortiGate is installed.

## What is the internal switch mode?

The internal switch mode determines how the FortiGate's physical ports are managed by the FortiGate. The two main modes are Switch mode and Interface mode.

## What are Switch mode and Interface mode and why are they used?

In Switch mode, all the internal interfaces are part of the same subnet and treated as a single interface, called either **lan** or **internal** by default, depending on the FortiGate model. Switch mode is used when the network layout is basic, with most users being on the same subnet.

In Interface mode, the physical interfaces of the FortiGate unit are handled individually, with each interface having its own IP address. Interfaces can also be combined by configuring them as part of either hardware or software switches, which allow multiple interfaces to be treated as a single interface. This mode is ideal for complex networks that use different subnets to compartmentalize the network traffic.

## Which mode is your FortiGate in by default?

The default mode that a FortiGate starts in varies depending on the model. To determine which mode your FortiGate unit is in, go to **System > Network > Interfaces**. Locate the **lan** or **internal** interface. If the interface is listed as a **Physical Interface** in the **Type** column, then your FortiGate is in Switch mode. If the interface is a **Hardware Switch**, then your FortiGate is in Interface mode.

## How do you change the mode?

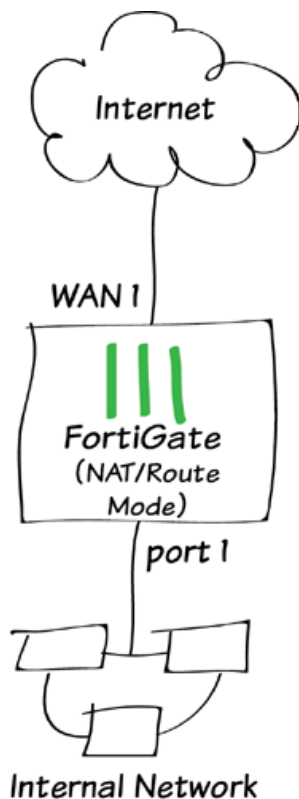
If you need to change the mode your FortiGate unit is in, first make sure that none of the physical ports that make up the **lan** or **internal** interface are referenced in the FortiGate configuration. Then go to **System > Dashboard > Status** and enter either of the following commands into the **CLI Console**:

1. Command to change the FortiGate to switch mode:

```
config system global
    set internal-switch-mode switch
exit
```
2. Command to change the FortiGate to interface mode:

```
config system global
    set internal-switch-mode interface
exit
```

# Installing a FortiGate in NAT/Route mode



In this example, you will learn how to connect and configure a new FortiGate unit in NAT/Route mode to securely connect a private network to the Internet.

In NAT/Route mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT).

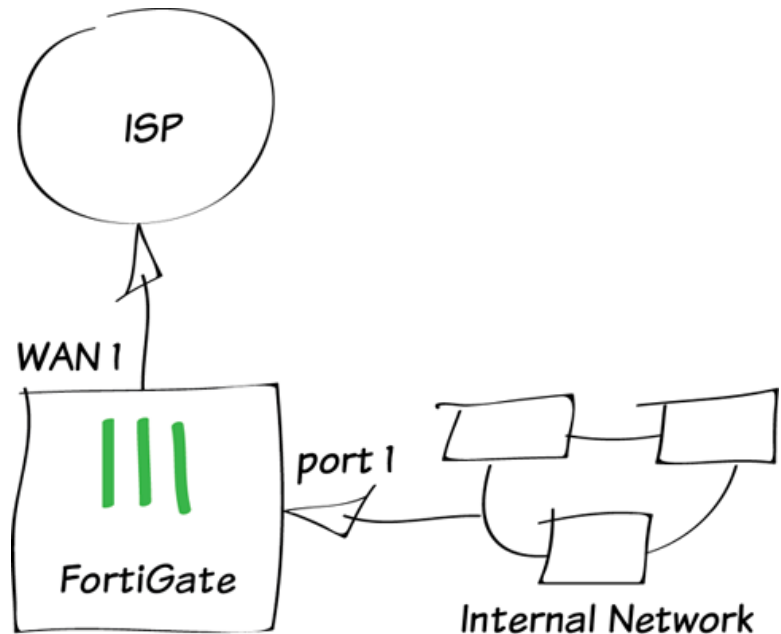
*If you have not already done so, ensure that your FortiGate is using the correct internal switch mode. For more information, see [Choosing your FortiGate's switch mode](#).*

A video of this recipe is available [here](#).

## 1. Connecting the network devices and logging onto the FortiGate

Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.



From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide).

Login using an admin account (the default admin account has the username admin and no password).

A screenshot of the FortiGate web-based manager login page. The background is a light gray with a subtle geometric pattern. In the center, there are two labels: 'Name' and 'Password'. To the right of 'Name' is a text input field containing the text 'admin'. To the right of 'Password' is an empty text input field. Below these fields is a red button with the word 'Login' in white text.

# 2. Configuring the FortiGate's interfaces

Go to **System > Network > Interfaces** and edit the Internet-facing interface.

If your FortiGate is directly connecting to your ISP, set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the public IP address your ISP has provided you with.

If have some ISP equipment between your FortiGate and the Internet (for example, a router), then the wan1 IP will also use a private IP assigned by the ISP equipment. If this equipment uses DHCP, set **Addressing Mode** to **DHCP** to get an IP assigned to the interface.

If the ISP equipment does not use DHCP, your ISP can provide you with the correct private IP to use for the interface.

Edit the **internal** interface (called **lan** on some FortiGate models).

Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.

|                 |   |
|-----------------|---|
| Interface Name  | wan1(08:5B:0E:31:74:13)   |
| Alias           | <input type="text"/>  |
| Link Status     | Up  |
| Type            | Physical Interface  |
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to Extension Device |
| IP/Network Mask | <input type="text" value="192.168.0.12/255.255.255.0"/>   |

|                 |   |
|-----------------|---|
| Interface Name  | internal(08:5B:0E:31:74:12)   |
| Alias           | <input type="text"/>  |
| Link Status     | Up  |
| Type            | Physical Interface  |
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to Extension Device |
| IP/Network Mask | <input type="text" value="172.20.120.99/255.255.255.0"/>  |

### 3. Adding a default route

Go to **Router > Static > Static Routes** (or **System > Network > Routing**, depending on your FortiGate model) and create a new route.

Set the **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.

*A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can edit it or delete it and add a new one.*

|                     |   |
|---------------------|---|
| Destination IP/Mask | <input type="text" value="0.0.0.0/0.0.0.0"/>          |
| Device              | <input type="text" value="wan1"/>                     |
| Gateway             | <input type="text" value="192.168.0.1"/>              |
| Distance            | <input type="text" value="10"/> (1-255, Default=10)   |
| Priority            | <input type="text" value="0"/> (0-4294967295)         |
| Comments            | <input type="text" value="Write a comment..."/> 0/255 |

### 4. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

|  |  |
|--|--|
| <b>DNS Settings</b>                          |  |
| <input type="radio"/> Use FortiGuard Servers | <input checked="" type="radio"/> Specify   |
| Primary DNS Server                           | <input type="text" value="208.91.123.53"/> |
| Secondary DNS Server                         | <input type="text" value="208.91.123.52"/> |
| Local Domain Name                            | <input type="text"/>                       |

## 5. Creating a policy to allow traffic from the internal network to the Internet

Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the **internal** interface and the **Outgoing Interface** to the Internet-facing interface.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected (later versions of FortiOS 5.2 call this option **Use Outgoing Interface Address**).

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Incoming Interface: internal

Source Address: all

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

☒ NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

**Logging Options**

☒ Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets























# 6. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

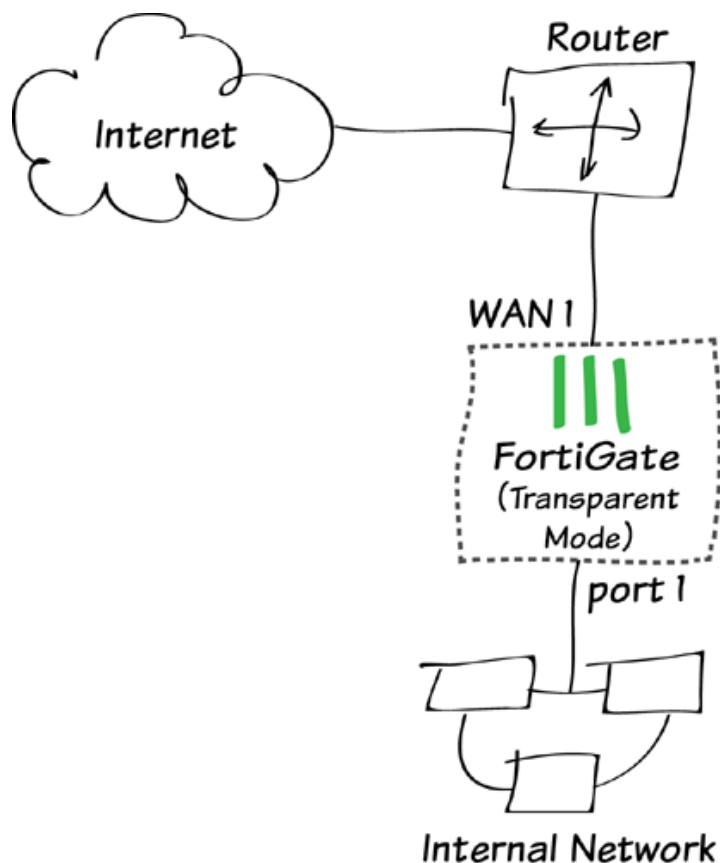
You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has the **internal** interface as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

If these two columns are not shown, right-click on the title row, select **Src Interface** and **Dst Interface** from the dropdown menu, and then select **Apply**.

| #  | Date/Time | Dst Interfa... | Src Interfa... | Destination   | Sent / Received    |
|----|-----------|----------------|----------------|---|--------------------|
| 1  | 13:10:25  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 1.10 KB / 640 B    |
| 2  | 13:10:25  | wan1           | lan            |  138.108.6.20 (secure-us.imrworldwide.com)       | 1.05 KB / 4.29 KB  |
| 3  | 13:10:24  | wan1           | lan            |  64.94.107.50 (map-pb.quantserve.com.akadns.net) | 967 B / 444 B      |
| 4  | 13:10:21  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 2.28 KB / 3.81 KB  |
| 5  | 13:10:21  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 3.34 KB / 5.83 KB  |
| 6  | 13:10:21  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 3.52 KB / 16.20 KB |
| 7  | 13:10:21  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 3.89 KB / 26.95 KB |
| 8  | 13:10:21  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 6.03 KB / 32.48 KB |
| 9  | 13:10:20  | wan1           | lan            |  208.91.114.158 (blog.fortinet.com)              | 1.26 KB / 2.22 KB  |
| 10 | 13:10:19  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 1.46 KB / 885 B    |
| 11 | 13:10:19  | wan1           | lan            |  64.94.107.50 (map-pb.quantserve.com.akadns.net) | 1.58 KB / 710 B    |
| 12 | 13:10:17  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 5.71 KB / 3.19 KB  |
| 13 | 13:10:17  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 5.54 KB / 3.19 KB  |
| 14 | 13:10:17  | wan1           | lan            |  194.122.82.32 (www.google.ca)                   | 184 B / 92 B       |
| 15 | 13:10:17  | wan1           | lan            |  194.122.82.32 (www.google.ca)                   | 184 B / 92 B       |
| 16 | 13:10:17  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 4.98 KB / 2.80 KB  |
| 17 | 13:10:17  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 8.01 KB / 4.69 KB  |
| 18 | 13:10:17  | wan1           | lan            |  8.247.14.128 (static.licdn.com)                 | 5.96 KB / 3.17 KB  |
| 19 | 13:10:16  | wan1           | lan            |  64.94.107.50 (map-pb.quantserve.com.akadns.net) | 1.02 KB / 496 B    |
| 20 | 13:10:16  | wan1           | lan            |  173.194.43.84 (www.google.com)                  | 272 B / 164 B      |

For further reading, check out [Installing a FortiGate in NAT/Route Mode](#) in the [FortiOS 5.2 Handbook](#).

# Installing a FortiGate in Transparent mode



In this example, you will learn how to connect and configure a new FortiGate unit in Transparent mode to securely connect a private network to the Internet. In Transparent mode, the FortiGate applies security scanning to traffic without applying routing or network address translation (NAT).

Warning: Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

A video of this recipe is available [here](#).

## 1. Changing the FortiGate's operation mode

Go to **System > Dashboard > Status** and locate the **System Information** widget.

Beside **Operation Mode**, select **Change**.

| System Information    |  |
|-----------------------|--|
| HA Status             | Standalone [Configure]                         |
| Host Name             | FG100D3G12812324 [Change]                      |
| Serial Number         | FG100D3G12812324                               |
| Operation Mode        | NAT [Change]                                   |
| System Time           | Tue Jul 15 09:04:33 2014 (FortiGuard) [Change] |
| Firmware Version      | v5.2.0,build0589 (GA) [Update] [Details]       |
| System Configuration  | [Backup] [Restore] [Revisions]                 |
| Current Administrator | admin [Change Password] / 1 in Total [Details] |
| Uptime                | 19 day(s) 2 hour(s) 14 min(s)                  |
| Virtual Domain        | Disabled [Enable]                              |

Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network.

|                       |                              |
|-----------------------|------------------------------|
| Operation Mode        | Transparent ▼                |
| Management IP/Netmask | 172.20.120.122/255.255.255.0 |
| Default Gateway       | 172.20.120.2                 |

You can now access the GUI by browsing to the Management IP (in the example, you would browse to *http://172.20.120.122*).

## 2. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

| DNS Settings                                 |  |
|--|--|
| <input type="radio"/> Use FortiGuard Servers | <input checked="" type="radio"/> Specify |
| Primary DNS Server                           | 208.91.123.53                            |
| Secondary DNS Server                         | 208.91.123.52                            |
| Local Domain Name                            |  |

### 3. Creating a policy to allow traffic from the internal network to the Internet

Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the an available external interface (typically port 1) and the **Outgoing Interface** to the Internet-facing interface (typically WAN1).

*It is recommended to avoid using any security profiles until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.*

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | port1           | + |
| Source Address      | all             | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | any             | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

**Logging Options**

☒ **Log Allowed Traffic**

☐ Security Events

☒ **All Sessions**

☐ Capture Packets

## 4. Connecting the network devices

Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.

Alternatively, you can enter the following command in the **CLI Console** (also found by going to **System > Dashboard > Status**):

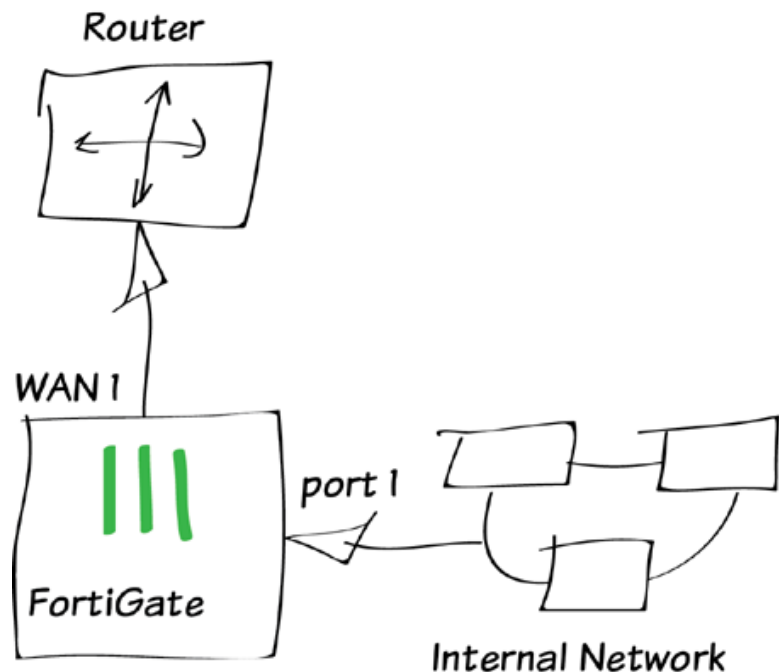
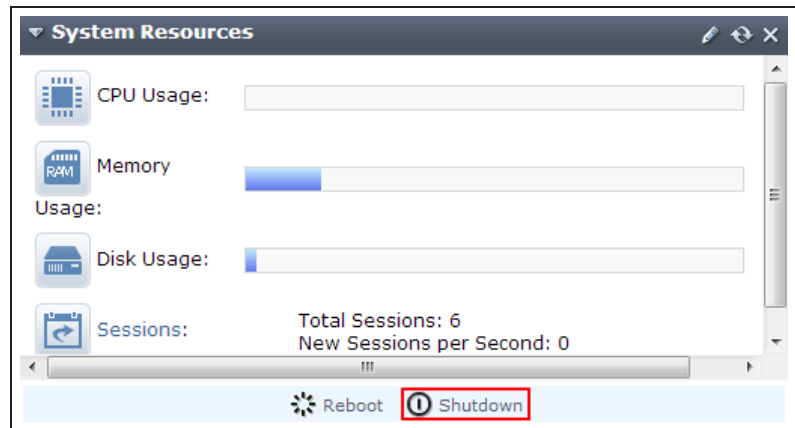
```
execute shutdown
```

Wait until all the lights, except for the power light, on your FortiGate have turned off. If your FortiGate has a power button, use it to turn the unit off. Otherwise, unplug the unit.

You can now connect the FortiGate unit between the internal network and the router.

Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.



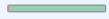


















Power on the FortiGate unit.



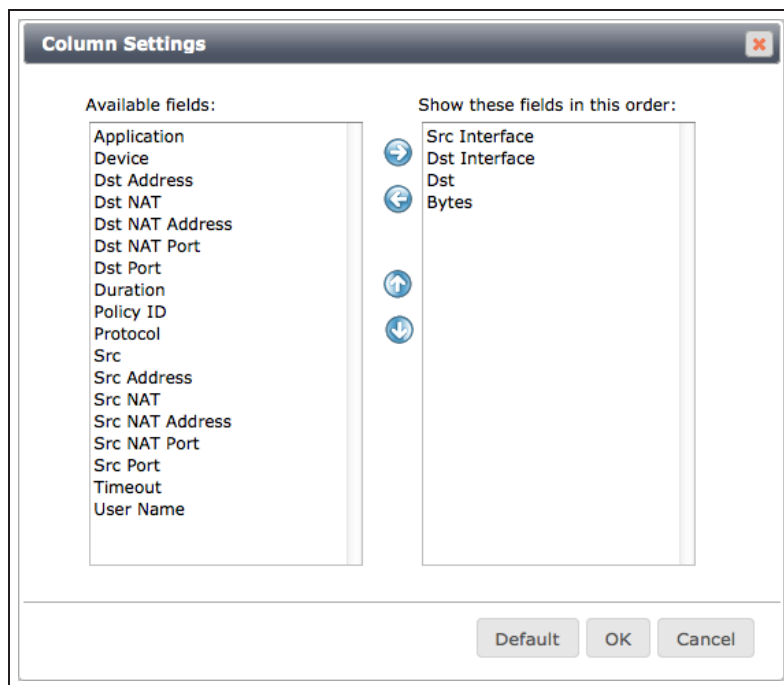
## 5. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has port 1 as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

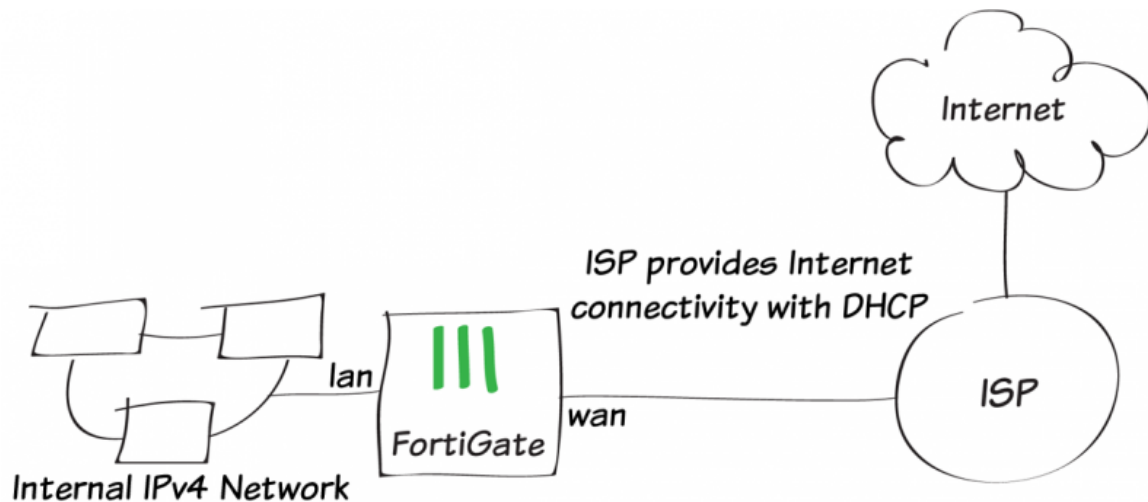
| #  | Src Interface | Dst Interface | Dst   | Bytes (Sent/Received)   |
|----|---------------|---------------|---|---|
| 1  | wan1          | wan1          | 172.20.120.122  | 6,567 I   |
| 2  | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 236 I   |
| 3  | port1         | wan1          |  s.yimg.com (68.142.250.160:443)                     | 1,026,162 I  |
| 4  | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 262 I   |
| 5  | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 291 I   |
| 6  | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 178 I   |
| 7  | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 204 I   |
| 8  | port1         | wan1          |  safebrowsing-cache.google.com (184.150.152.152:443) | 10,721 I  |
| 9  | port1         | wan1          |  BN1WNS1011410.wns.windows.com (157.56.98.65:443)    | 7,903 I   |
| 10 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 211 I   |
| 11 | port1         | wan1          |  google-public-dns-a.google.com (8.8.8.8:53)         | 385 I   |
| 12 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 226 I   |
| 13 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 173 I   |
| 14 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 413 I   |
| 15 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 204 I   |
| 16 | port1         | wan1          |  safebrowsing-cache.google.com (184.150.152.178:443) | 876,026 I    |
| 17 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 184 I   |
| 18 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 441 I   |
| 19 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 212 I   |
| 20 | port1         | wan1          |  google-public-dns-b.google.com (8.8.4.4:53)         | 204 I   |

If these two columns are not shown, select **Column Settings** and move **Src Interface** and **Dst Interface** to the list of fields to be shown.



For further reading, check out [Installation](#) in the [FortiOS 5.2 Handbook](#).

# Quick installation using DHCP



In this example, you will use DHCP and your FortiGate's default configuration to securely connect your internal network to the Internet in two simple steps.

This recipe has the following requirements:

- An ISP that provides connectivity with DHCP and accepts DHCP requests without authentication.
- A FortiGate with a default configuration that includes a DHCP server on the lan (or internal) interface and a security policy that securely allows all sessions from the Internal network to reach the Internet.
- Your network uses IPv4 to connect to the FortiGate and Internet.

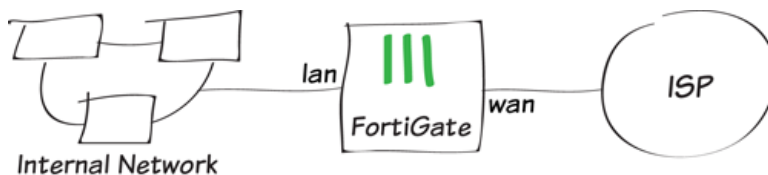


## 1. Connecting the FortiGate to your ISP and the internal network

Connect the FortiGate **wan** interface to your ISP-supplied equipment.

Connect the internal network to the FortiGate's default **lan** or **internal** interface.

Turn on the ISP's equipment, the FortiGate unit, and the PCs on the internal network.



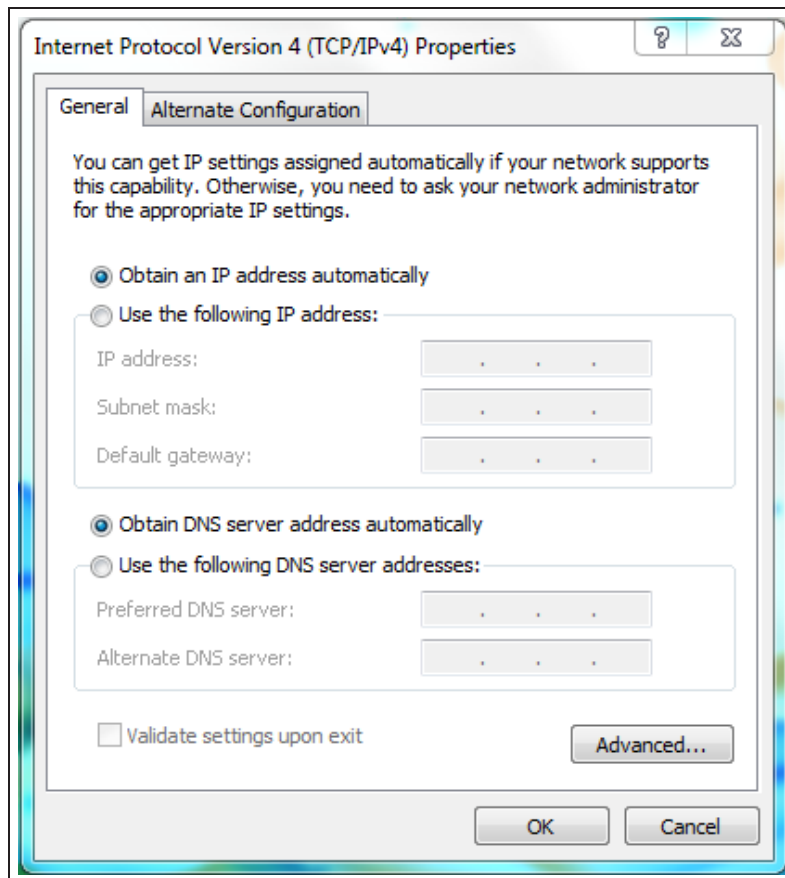
## 2. Configuring your PCs to use DHCP

Windows Vista/7/8:

Go to **Network and Sharing Center** and select **Local Area Connections**. Select **Properties**.

Select **Internet Protocol Version 4 (TCP/IPv4)**, then select **Properties**.

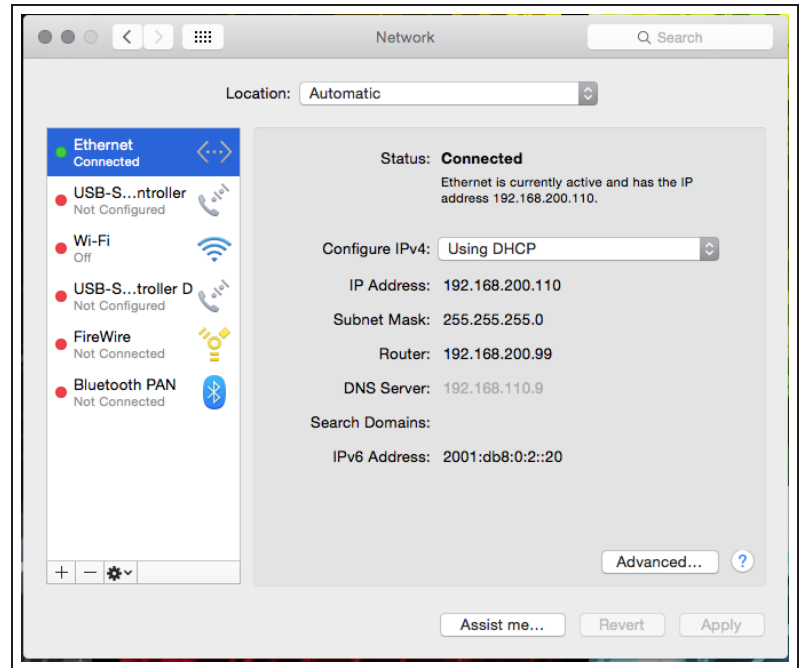
Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



## Mac OS X

Go to **Network Preferences** and select **Ethernet**.

Set **Configure IPv4** to **Using DHCP**.



### 3. Results

From any PC on the internal network, open a web browser and browse to any website. You can successfully connect to the Internet.

| Seq.#              | Source | Destination | Action   | NAT      | Log | Count                       |
|--------------------|--------|-------------|----------|----------|-----|-----------------------------|
| lan - wan1 (1 - 1) |        |             |          |          |     |                             |
| 1                  | all    | all         | ✓ ACCEPT | ✓ Enable | UTM | 5,075,951 Packets / 2.89 GB |

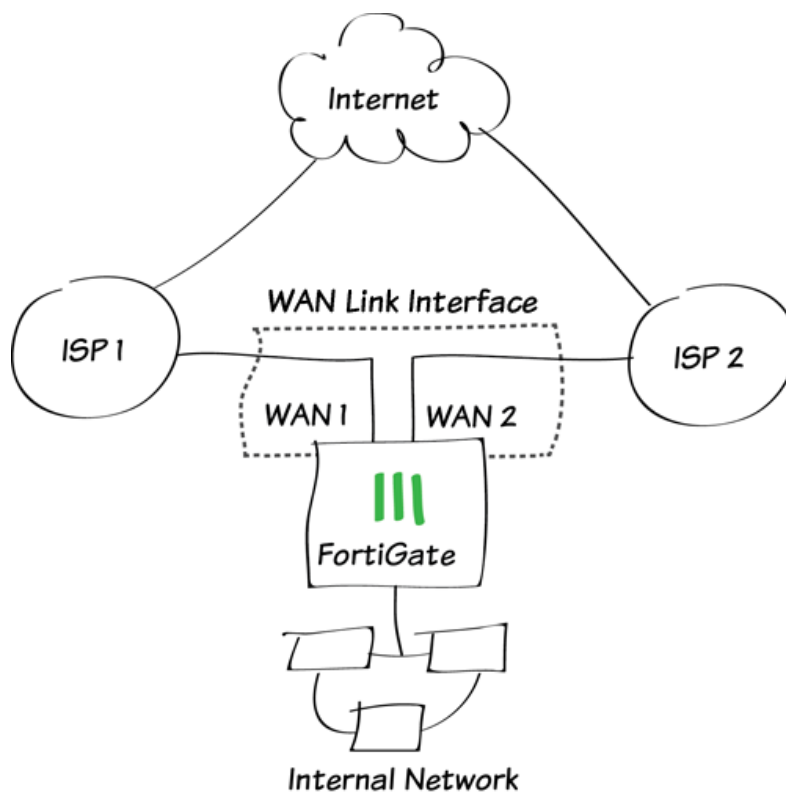
Go to **Policy & Objects > IPv4 > Policy**. Your Internet-access policy is at the top of list, in the **lan - wan** section (this section's name varies based on the FortiGate model).

View the **Count** column, which displays the total amount of traffic that has used this policy since the FortiGate's last reboot. The column should display results, showing that the policy is being used for traffic.

If this column is not visible, right-click on the title row, select **Count**, then **Apply**.

For further reading, check out [Installation](#) in the [FortiOS 5.2 Handbook](#).

# Redundant Internet connections



In this example, you will create a WAN link interface that provides your FortiGate unit with redundant Internet connections from two Internet service providers (ISPs). The WAN link interface combines these two connections into a single interface.

This example includes weighted load balancing so that most of your Internet traffic is handled by one ISP.

A video of this recipe can be found [here](#).

## 1. Connecting your ISPs to the FortiGate

Connect your ISP devices to your FortiGate so that the ISP you wish to use for most traffic is connected to WAN1 and the other connects to WAN2.



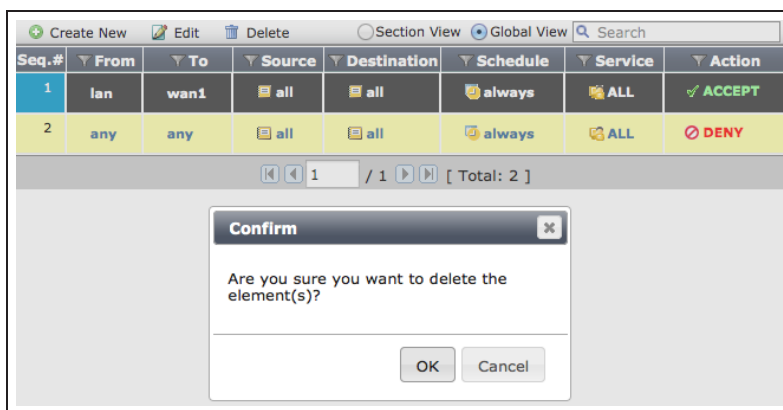
## 2. Deleting security policies and routes that use WAN1 or WAN2

You will not be able to add an interface to the WAN link interface if it is already used in the FortiGate's configuration, so you must delete any policies or routes that use either WAN1 or WAN2.

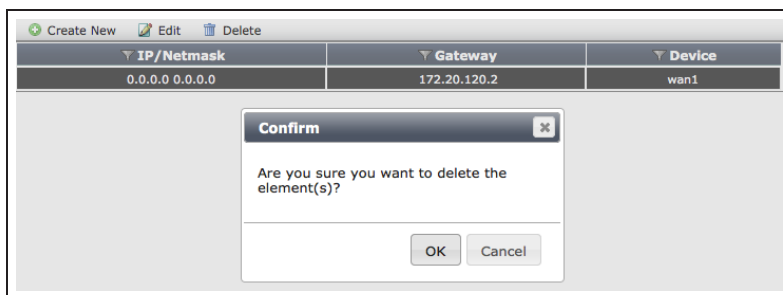
Many FortiGate models include a default Internet access policy that uses WAN1. This policy must also be deleted.

Go to **Policy & Objects > Policy > IPv4** and delete any policies that use WAN1 or WAN2.

*After you remove these policies, traffic will no longer be able to reach WAN1 or WAN2 through the FortiGate.*



Go to **Router > Static > Static Routes** and delete any routes that use WAN1 or WAN2.



### 3. Creating a WAN link interface

Go to **System > Network > WAN Link Load Balancing**.

Set **WAN Load Balancing** to **Weighted Round Robin**. This will allow you to prioritize the WAN1 interface so that more traffic uses it.

Add WAN1 to the list of **Interface Members**, set **Weight** to 3, and set it to use the **Gateway IP** provided by your ISP.

You can optionally configure **Health Check** to verify that WAN1 can connect to the Internet.

| Name                      | wan-load-balance  |           |              |        |         |                           |  |  |  |
|---------------------------|---|-----------|--------------|--------|---------|---------------------------|--|--|--|
| Type                      | WAN Link Load Balancing Interface   |           |              |        |         |                           |  |  |  |
| WAN Load Balancing        | <input type="radio"/> Source IP based <input checked="" type="radio"/> Weighted Round Robin <input type="radio"/> Spill-over <input type="radio"/> Source-Destination   |           |              |        |         |                           |  |  |  |
| Interface Members         | <div><a href="#">Create New</a> <a href="#">Edit</a> <a href="#">Delete</a></div> <table><thead><tr><th>Interface</th><th>Probe Server</th><th>Weight</th><th>Gateway</th></tr></thead><tbody><tr><td colspan="4">No matching entries found</td></tr></tbody></table> | Interface | Probe Server | Weight | Gateway | No matching entries found |  |  |  |
| Interface                 | Probe Server  | Weight    | Gateway      |        |         |                           |  |  |  |
| No matching entries found |   |           |              |        |         |                           |  |  |  |

|  |              |
|--|--------------|
| Interfaces                                       | wan1         |
| Weight   | 3            |
| Gateway IP                                       | 172.20.120.2 |
| <input checked="" type="checkbox"/> Health Check |              |
| Probe Type                                       | Ping         |
| Probe Server                                     | 172.20.120.2 |
| Probe Interval (s)                               | 5            |
| Failure Threshold                                | 5            |
| Recovery Threshold                               | 5            |

Do the same for WAN2, but instead set **Weight** to 1.

You can optionally configure **Health Check** to verify that WAN2 can connect to the Internet.

The weight settings will cause 75% of traffic to use WAN1, with the remaining 25% using WAN2.

|  |              |
|--|--------------|
| Interfaces                                       | wan2         |
| Weight   | 1            |
| Gateway IP                                       | 182.20.120.2 |
| <input checked="" type="checkbox"/> Health Check |              |
| Probe Type                                       | Ping         |
| Probe Server                                     | 182.20.120.2 |
| Probe Interval (s)                               | 5            |
| Failure Threshold                                | 5            |
| Recovery Threshold                               | 5            |

## 4. Creating a default route for the WAN link interface

Go to **Router > Static > Static Routes** and create a new default route.

Set **Device** to the WAN link interface.

|                     |   |
|---------------------|---|
| Destination IP/Mask | <input type="text" value="0.0.0.0/0.0.0.0"/>          |
| Device              | <input type="text" value="wan-load-balance"/>         |
| Distance            | <input type="text" value="10"/> (1-255, Default=10)   |
| Priority            | <input type="text" value="0"/> (0-4294967295)         |
| Comments            | <input type="text" value="Write a comment..."/> 0/255 |

## 5. Allowing traffic from the internal network to the WAN link interface

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your internal network's interface and set **Outgoing Interface** to the WAN link interface.

Turn on **NAT**.

|                     |   |
|---------------------|---|
| Incoming Interface  | <input type="text" value="lan"/>              |
| Source Address      | <input type="text" value="all"/>              |
| Source User(s)      | <input type="text" value="Click to add..."/>  |
| Source Device Type  | <input type="text" value="Click to add..."/>  |
| Outgoing Interface  | <input type="text" value="wan-load-balance"/> |
| Destination Address | <input type="text" value="all"/>              |
| Schedule            | <input type="text" value="always"/>           |
| Service             | <input type="text" value="ALL"/>              |
| Action              | <input type="text" value="ACCEPT"/>           |

**Firewall / Network Options**

☒ NAT

☒ Use Destination Interface Address ☐ Fixed Port

Scroll down to view the Logging Options. To view the results later, turn on Log Allowed Traffic and select All Sessions.

**Logging Options**

☒ Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets





## 6. Results

Browse the Internet using a PC on the internal network and then go to **System > FortiView > All Sessions**.

Ensure that the **Dst Interface** column is visible in the traffic log. If it is not shown, right-click on the title row and select **Dst Interface** from the dropdown menu. Scroll to the bottom of the menu and select **Apply**.

The log shows traffic flowing through both WAN1 and WAN2.

Disconnect the WAN1 port, continue to browse the Internet, and refresh the traffic log. All traffic is now flowing through WAN2, until you reconnect WAN1.

| # | Src Interface | Src                   | Dst Interface | Bytes (Sent/Received)   |
|---|---------------|-----------------------|---------------|---|
| 1 | lan           | 192.168.200.114:54819 | wan2          | 50,909   |
| 2 | lan           | 192.168.200.114:54835 | wan1          | 50,839   |
| 3 | lan           | 192.168.200.114:54803 | wan2          | 69,529   |
| 4 | lan           | 192.168.200.114:54787 | wan1          | 257,587  |
| 5 | lan           | 192.168.200.114:54891 | wan1          | 1,971   |
| 6 | lan           | 192.168.200.114:54987 | wan2          | 1,436   |
| 7 | lan           | 192.168.200.114:54931 | wan1          | 3,086   |

| # | Src Interface | Src                   | Dst Interface | Bytes (Sent/Received) |
|---|---------------|-----------------------|---------------|-----------------------|
| 1 | lan           | 192.168.200.114:55491 | wan2          | 286                   |
| 2 | lan           | 192.168.200.114:63123 | wan2          | 365                   |
| 3 | lan           | 192.168.200.114:34499 | wan2          | 434                   |
| 4 | lan           | 192.168.200.114:35923 | wan2          | 362                   |
| 5 | lan           | 192.168.200.114:37443 | wan2          | 353                   |
| 6 | lan           | 192.168.200.114:63555 | wan2          | 100                   |

For further reading, check out [Installing a FortiGate in NAT/Route Mode](#) in the [FortiOS 5.2 Handbook](#).



# Troubleshooting your FortiGate installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods.

Most methods can be used for both FortiGates in both NAT/Route and Transparent mode. Any exceptions are marked.

## Use FortiExplorer if you can't connect to the FortiGate over Ethernet.

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's [QuickStart Guide](#) for details.

## Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.

## Check the physical network connections.

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device. Also, check the Unit Operation widget, found at **System > Dashboard > Status**, to make sure the connected interfaces are shown in green.

## Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).

Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.

If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.

## Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

## Check the FortiGate interface configurations (NAT/Route mode).

Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure **Addressing Mode** is set to the correct mode.

## Verify the security policy configuration.

Go to **Policy & Objects > Policy > IPv4** (or **Policy & Objects > Policy > IPv6**) and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Sessions**, and select **Apply**).

If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is turned on and that **Use Destination Interface Address** is selected (later versions of FortiOS 5.2 call this option **Use Outgoing Interface Address**).

## Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).

Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to Internet-facing interface.

## Verify the static routing configuration (NAT/Route mode).

Go to **Router > Static > Static Routes** (or **System > Network > Routing**) and verify that the default route is correct. View the **Routing Monitor** (found either on the same page or at **Router > Monitor > Routing Monitor**) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.

## Verify that you can connect to the gateway provided by your ISP.

Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

## Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

## Verify the DNS configurations of the FortiGate unit and the PCs.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`. If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

## Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, confirm that it can reach FortiGuard.

First, check the License Information widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to **System > Config > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the GUI should show a successful connection.

## Consider changing the MAC address of your external interface (NAT/Route mode).

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
  edit
    set macaddr
  end
end
```

## Check the FortiGate bridge table (Transparent mode).

When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit. Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed that is a likely cause. Check for the MAC address of the interface or device in question.

To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. Check the device's network connections and make sure they are connected and operational.

## Either reset the FortiGate unit to factory defaults or contact the technical assistance center.

If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

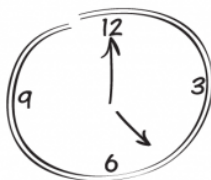
*Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.*

You can also contact the technical assistance center. For contact information, go to [support.fortinet.com](https://support.fortinet.com).

# FortiGate registration and basic settings



***Register your  
FortiGate***



***Set the  
system time***



***Configure the  
admin account***

In this example, you will register your FortiGate unit and set the system time. You will also configure several administrative account settings to prevent unauthorized access.

# 1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to **Fortinet Support**.

Before registering your FortiGate unit, it must have Internet connectivity.

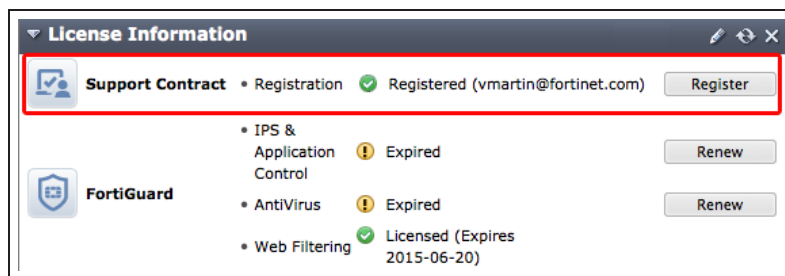
Go to **System > Dashboard > Status** and locate the **License Information** widget.

Next to **Support Contract**, select **Register**.

Either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.

*It is recommend to use a common account to register all your Fortinet products, to allow the Support site to keep a complete listing of your devices.*

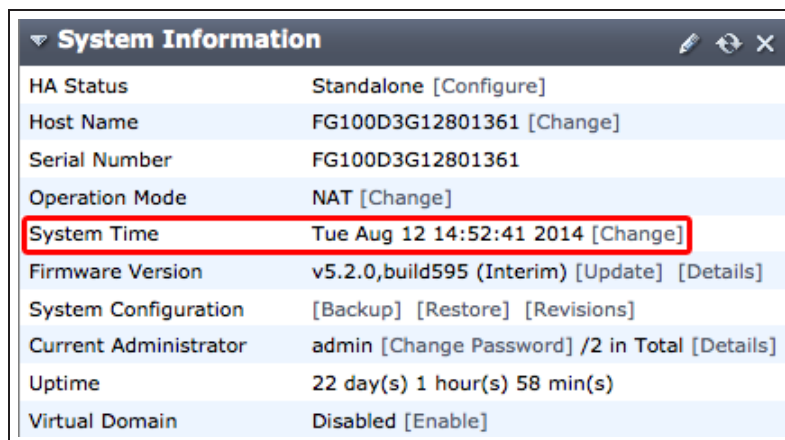
The **License Information** widget now displays the unit as **Registered**.



## 2. Setting the system time

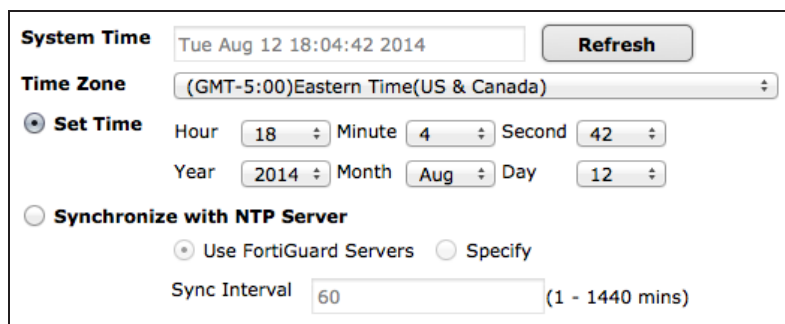
Go to **System > Dashboard > Status** and locate the **System Information** widget.

Next to **System Time**, select **Change**.



Select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.

*Since not all time zones have names, you may need to know how many hours ahead (+) or behind (-) you are from Greenwich Mean Time (GMT).*



The **System Information** widget now displays the correct time.

| System Information    |   |
|-----------------------|---|
| HA Status             | Standalone [Configure]                        |
| Host Name             | FG100D3G12801361 [Change]                     |
| Serial Number         | FG100D3G12801361                              |
| Operation Mode        | NAT [Change]                                  |
| System Time           | Tue Aug 12 18:04:49 2014 [Change]             |
| Firmware Version      | v5.2.0,build595 (Interim) [Update] [Details]  |
| System Configuration  | [Backup] [Restore] [Revisions]                |
| Current Administrator | admin [Change Password] /2 in Total [Details] |
| Uptime                | 22 day(s) 1 hour(s) 58 min(s)                 |
| Virtual Domain        | Disabled [Enable]                             |

### 3. (Optional) Restricting administrative access to a trusted host

Go to **System > Admin > Administrators** and edit the default *admin* account.

Enable **Restrict this Administrator Login from Trusted Hosts Only**. Set **Trusted Host #1** to the static IP address of the PC you will use to administer the FortiGate unit, using /32 as the netmask.

You can also set an entire subnet as the trusted host, using /24 as the netmask.

If required, set additional trusted hosts.

☒ Restrict this Administrator Login from Trusted Hosts Only

|                      |                    |
|----------------------|--------------------|
| Trusted Host #1      | 192.168.220.110/32 |
| Trusted Host #2      | 0.0.0.0/0.0.0.0    |
| Trusted Host #3      | 0.0.0.0/0.0.0.0    |
| IPv6 Trusted Host #1 | ::/0               |
| IPv6 Trusted Host #2 | ::/0               |
| IPv6 Trusted Host #3 | ::/0               |

### 4. Changing the default admin password

Go to **System > Admin > Administrators** and edit the default *admin* account.

Select **Change Password**. Leave **Old Password** blank and enter the **New Password**.

You will be automatically signed out after changing the password.

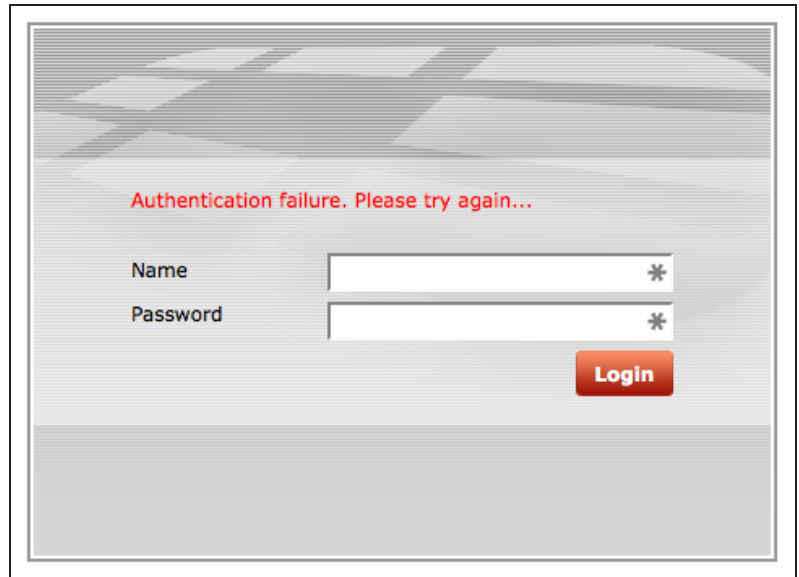
|                  |                          |
|------------------|--------------------------|
| Administrator    | admin                    |
| Old Password     | <input type="password"/> |
| New Password     | <input type="password"/> |
| Confirm Password | <input type="password"/> |



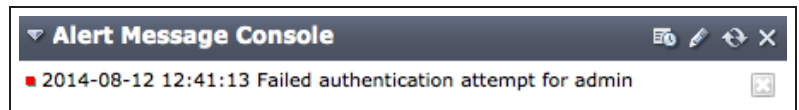
## 5. Results

Attempt to log in using the admin account without a password. Access is denied.

Log in using the new password to access the FortiGate.



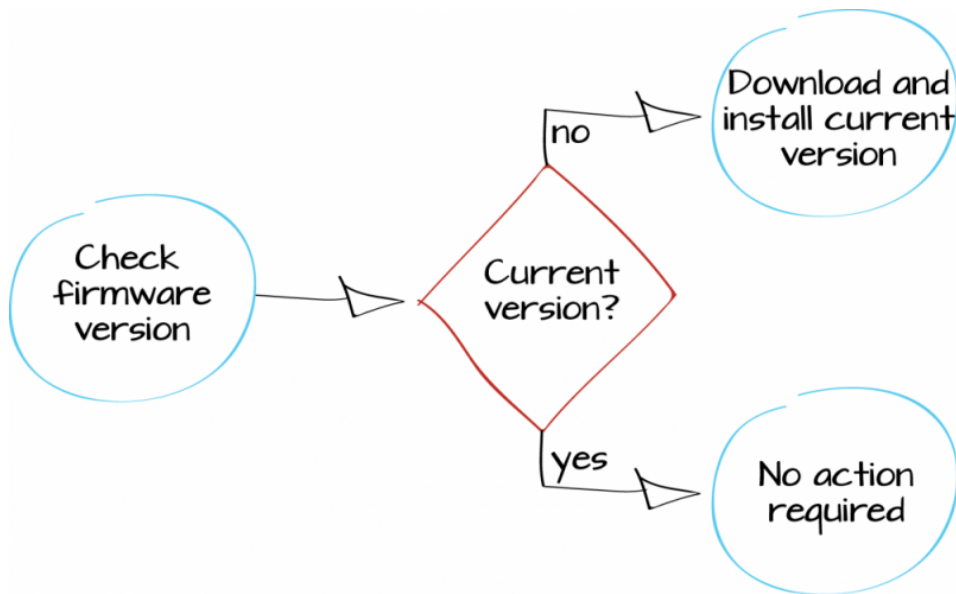
Go to **System > Dashboard > Status** and locate the **Alert Message Console** widget, which indicates the failed authentication attempt.



(Optional) If access has been restricted to a trusted host, attempts to connect from a device that is not trusted will be denied.

For further reading, check out [Basic Administration](#) in the [FortiOS 5.2 Handbook](#).

# Updating your FortiGate's firmware



This example verifies the current version of FortiOS firmware and, if necessary, updates it to the latest version.

FortiOS is the operating system used by FortiGate and FortiWiFi units. You can update FortiOS to use the latest tools and security features available.

## 1. Checking the current FortiOS firmware

Log in to the GUI and go to **System > Dashboard > Status** and view the **System Information** dashboard widget. The **Firmware Version** section shows the firmware that is currently installed and if a new version is available.

| System Information    |   |
|-----------------------|---|
| HA Status             | Standalone [Configure]  |
| Host Name             | FG100D3G12812324 [Change]   |
| Serial Number         | FG100D3G12812324  |
| Operation Mode        | NAT [Change]  |
| System Time           | Wed Apr 8 10:38:55 2015 (FortiGuard) [Change]   |
| Firmware Version      | v5.2.2,build642 (GA) [Update]<br>⚠ A new firmware version is available (5.2.3) [View Release Notes] |
| System Configuration  | [Backup] [Restore] [Revisions]  |
| Current Administrator | admin [Change Password] / 1 in Total [Details]  |
| Uptime                | 18 day(s) 21 hour(s) 2 min(s)   |
| Virtual Domain        | Disabled [Enable]   |

## 2. Reviewing the Release Notes

If a new version is available, select **View Release Notes** to access the Release Notes for that version. Review the release notes to determine if you want to upgrade to this version.

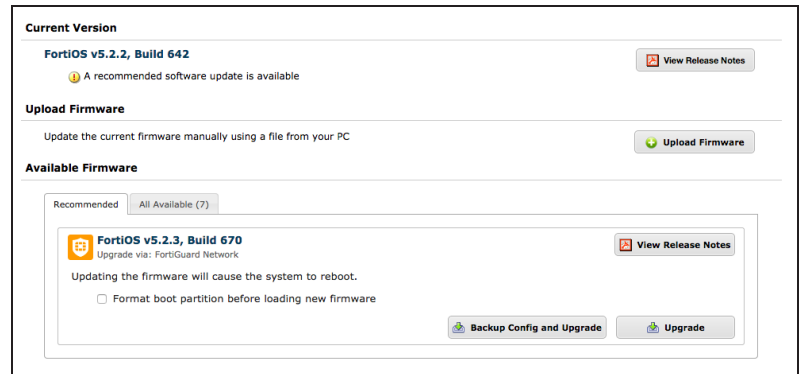
Pay extra attention to the **Upgrade Information** section, to find out if you can upgrade directly from your current firmware to the latest version. You should also check the **Supported Upgrade Paths** document, found at the [Fortinet Documentation Library](#).



### 3. Updating to the latest firmware

If you wish to upgrade to the latest FortiOS version, select **Update**.

Under **Available Firmware**, select the **Recommended** tab, then select **Backup Config and Upgrade**.



### 4. Results

The FortiGate unit uploads the firmware image file, updates to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

You may have to refresh your browser to see the FortiGate login.

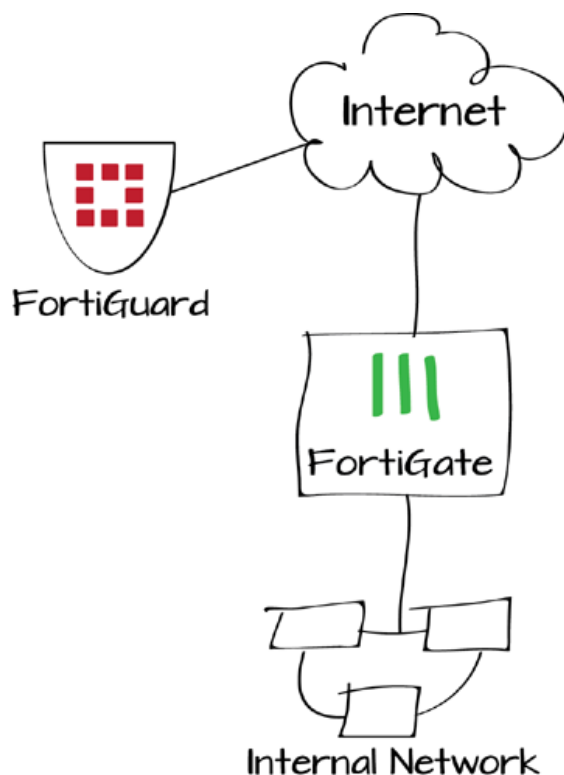


Go to **System > Dashboard > Status**.  
In the **System Information** dashboard widget, the **Firmware Version** will show the updated version of FortiOS.

| System Information    |   |
|-----------------------|---|
| HA Status             | Standalone [Configure]                        |
| Host Name             | FG100D3G12812324 [Change]                     |
| Serial Number         | FG100D3G12812324                              |
| Operation Mode        | NAT [Change]                                  |
| System Time           | Wed Apr 8 10:52:30 2015 (FortiGuard) [Change] |
| Firmware Version      | v5.2.3,build670 (GA) [Update]                 |
| System Configuration  | [Backup] [Restore] [Revisions]                |
| Current Administrator | admin [Change Password] /1 in Total [Details] |
| Uptime                | 0 day(s) 0 hour(s) 3 min(s)                   |
| Virtual Domain        | Disabled [Enable]                             |

For further reading, check out **Firmware** in the **FortiOS 5.2 Handbook**.

# Setting up FortiGuard services



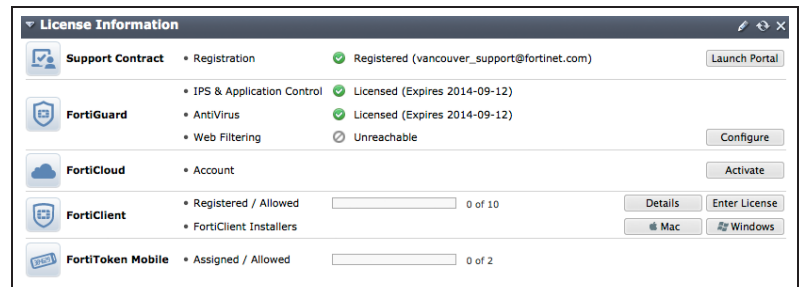
If you have purchased FortiGuard services and registered your FortiGate unit, the FortiGate should automatically connect to FortiGuard and display license information about your FortiGuard services. In this example, you will verify whether the FortiGate unit is communicating with the FortiGuard Distribution Network (FDN) by checking the **License Information** dashboard widget.

## 1. Verifying the connection

Go to **System > Dashboard > Status** and go to the **License Information** widget. Any subscribed services should have a green checkmark, indicating that connections are successful.

A gray X indicates that the FortiGate unit cannot connect to the FortiGuard network, or that the FortiGate unit is not registered.

A red X indicates that the FortiGate unit was able to connect but that a subscription has expired or has not been activated.



You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.

|                                    |   |   |
|------------------------------------|---|---|
| <b>Support Contract</b>            |   |   |
| Registration                       | Registered (Login ID: vancouver_support@fortinet.com) <a href="#">[Login Now]</a> | ✓ |
| Hardware                           | 8 x 5 support (Expires: 2014-09-12)   | ✓ |
| Firmware                           | 8 x 5 support (Expires: 2014-09-12)   | ✓ |
| Enhanced Support                   | 24 x 7 support (Expires: 2014-09-12)  | ✓ |
| Comprehensive Support              | 24 x 7 support (Expires: 2014-09-12)  | ✓ |
| <b>FortiGuard Services</b>         |   |   |
| <b>Next Generation Firewall</b>    |   |   |
| IPS & Application Control          | Licensed (Expires 2014-09-12)   | ✓ |
| IPS Definitions                    | 4.00444 (Updated 2014-03-26 via Manual Update) <a href="#">[Update]</a>           |   |
| IPS Engine                         | 3.00038 (Updated 2014-06-11 via Manual Update)                                    |   |
| <b>ATP Services</b>                |   |   |
| AntiVirus                          | Licensed (Expires 2014-09-12)   | ✓ |
| AV Definitions                     | 1.00000 (Updated 2012-10-17 via Manual Update) <a href="#">[Update]</a>           |   |
| AV Engine                          | 5.00154 (Updated 2014-06-11 via Manual Update)                                    |   |
| Web Filtering                      | Unreachable   | ✗ |
| <b>Other Services</b>              |   |   |
| Vulnerability Scan                 | Licensed (Expires 2014-09-12)   | ✓ |
| VCM Plugins                        | 1.00366 (Updated 2014-07-09 via Manual Update) <a href="#">[Update]</a>           |   |
| Email Filtering                    | Unreachable   | ✗ |
| Messaging Services                 | Unreachable   | ✗ |
| <b>FortiClient Information</b>     |   |   |
| FortiGuard Availability            | Reachable   | ✓ |
| FortiClient Version (Mac)          | 5.2.0 (Updated 2014-07-14)  |   |
| FortiClient Version (Windows)      | 5.2.0 (Updated 2014-07-14)  |   |
| <b>SSL-VPN Package Information</b> |   |   |
| SSL-VPN Package Version            | 4.0.2292 (Updated 2013-11-01)   |   |
| <b>FortiToken Seed Server</b>      |   |   |
| Registration                       | Reachable (0 Tokens Registered)   | ✓ |



## 2. Troubleshooting communication errors

Go to **System > Network > DNS** and ensure that the primary and secondary DNS servers are correct.

*In this screenshot, the FortiGate has been successfully tested already.*

**DNS Settings**

**DNS Settings**

☒ Use FortiGuard Servers ☐ Specify

Primary DNS Server

Secondary DNS Server

Local Domain Name

Connected to FortiGuard ☒

Web Filtering Licensed ☒

☐ Enable FortiGuard DDNS

**Apply**

To test if you are connected to the correct DNS server, go to **System > Dashboard > Status** and enter the following command into the CLI Console:

```
execute ping guard.fortinet.net
```

If the connection is successful, the CLI Console should display a similar output as the example.

```
CLI Console
Connected

FGT60C3G10016011 # execute ping guard.fortinet.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=52 time=62.3 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=52 time=62.6 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=52 time=61.5 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=52 time=61.7 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=52 time=61.3 ms

--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 61.3/61.8/62.6 ms
```

To test if the FortiGuard services are reachable, go to **System > Config > FortiGuard**.

Under the **Web Filtering and Email Filtering Options**, select **Test Availability**. This will indicate which ports are open. If the FortiGate default port (53) cannot be unblocked, go to **System > Config > FortiGuard**. Under the **Web Filtering and Email Filtering Options** choose **Use Alternate Port (8888)**.

*If you are updating FortiGuard using a FortiManager, the FortiGate can also use port 80.*

If further problems occur, you may have to unblock ports using the CLI. See the [CLI Reference for FortiOS 5.2](#) for more information.

### 3. Results

Go to **System > Dashboard > Status** and go to the **License Information** widget.

Any subscribed services should have a green checkmark, indicating that connections have been established and that the licenses have been verified.

FortiClient Information

FortiGuard Availability

Reachable

✓

FortiClient Version (Mac)

5.2.0 (Updated 2014-07-15)

FortiClient Version (Windows)

5.2.0 (Updated 2014-07-15)

SSL-VPN Package Information

SSL-VPN Package Version

4.0.2292 (Updated 2013-11-01)

FortiToken Seed Server

Registration

Reachable (0 Tokens Registered)

✓

AV & IPS Download Options

Web Filtering and Email Filtering Options

Enable webfilter cache

TTL: 3600

Enable antispam cache

TTL: 1800

Port Selection

Use Default Port (53)

Use Alternate Port (8888)

Test Availability

(FortiGuard services are reachable via ports 53 and 8888.)

To have a URL's category rating re-evaluated, [please click here.](#)

Apply

License Information

Support Contract

Registration

Registered

(vancouver\_support@fortinet.com)

Launch Portal

FortiGuard

IPS & Application Control

AntiVirus

Web Filtering

Licensed (Expires 2014-09-12)

Licensed (Expires 2014-09-12)

Licensed (Expires 2014-09-12)

FortiCloud

Account

Activate

FortiClient

Registered / Allowed

0 of 10

Details

Enter License

Mac

Windows

FortiToken Mobile

Assigned / Allowed

0 of 2

Go to **System > Config > FortiGuard**.

Features and services you are subscribed to should have a green checkmark, indicating that connections are successful.

|                                    |   |   |
|------------------------------------|---|---|
| <b>Support Contract</b>            |   |   |
| Registration                       | Registered (Login ID: vancouver_support@fortinet.com) <a href="#">[Login Now]</a> | ✓ |
| Hardware                           | 8 x 5 support (Expires: 2014-09-12)   | ✓ |
| Firmware                           | 8 x 5 support (Expires: 2014-09-12)   | ✓ |
| Enhanced Support                   | 24 x 7 support (Expires: 2014-09-12)  | ✓ |
| Comprehensive Support              | 24 x 7 support (Expires: 2014-09-12)  | ✓ |
| <b>FortiGuard Services</b>         |   |   |
| <b>Next Generation Firewall</b>    |   |   |
| IPS & Application Control          | Licensed (Expires 2014-09-12)   | ✓ |
| IPS Definitions                    | 4.00444 (Updated 2014-03-26 via Manual Update) <a href="#">[Update]</a>           |   |
| IPS Engine                         | 3.00038 (Updated 2014-06-11 via Manual Update)                                    |   |
| =====                              |   |   |
| <b>ATP Services</b>                |   |   |
| AntiVirus                          | Licensed (Expires 2014-09-12)   | ✓ |
| AV Definitions                     | 1.00000 (Updated 2012-10-17 via Manual Update) <a href="#">[Update]</a>           |   |
| AV Engine                          | 5.00154 (Updated 2014-06-11 via Manual Update)                                    |   |
| Web Filtering                      | Licensed (Expires 2014-09-12)   | ✓ |
| =====                              |   |   |
| <b>Other Services</b>              |   |   |
| Vulnerability Scan                 | Licensed (Expires 2014-09-12)   | ✓ |
| VCM Plugins                        | 1.00366 (Updated 2014-07-09 via Manual Update) <a href="#">[Update]</a>           |   |
| Email Filtering                    | Licensed (Expires 2014-09-12)   | ✓ |
| Messaging Services                 | Licensed (Expires 2014-09-12)   | ✓ |
| =====                              |   |   |
| <b>FortiClient Information</b>     |   |   |
| FortiGuard Availability            | Reachable   | ✓ |
| FortiClient Version (Mac)          | 5.2.0 (Updated 2014-07-16)  |   |
| FortiClient Version (Windows)      | 5.2.0 (Updated 2014-07-16)  |   |
| <b>SSL-VPN Package Information</b> |   |   |
| SSL-VPN Package Version            | 4.0.2292 (Updated 2013-11-01)   |   |
| <b>FortiToken Seed Server</b>      |   |   |
| Registration                       | Reachable (0 Tokens Registered)   | ✓ |

For further reading, check out **FortiGuard** in the **FortiOS 5.2 Handbook**.

# FortiGuard troubleshooting

This section contains tips to help you with some common challenges of using FortiGuard.

## FortiGuard services appear as expired/unreachable.

Verify that you have registered your FortiGate unit, purchased FortiGuard services and that the services have not expired at [support.fortinet.com](https://support.fortinet.com).

## Services are active but still appear as expired/unreachable.

Verify that the FortiGate unit can communicate with the Internet by accessing FortiGate CLI and using the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

## The FortiGate is connected to the Internet but can't communicate with FortiGuard.

If you have not done so already, verify your DNS settings and ensure that an unblocked port is being used for FortiGuard traffic.

If the FortiGate interface connected to the Internet gets its IP address using DHCP, go to **System > Network > Interfaces** and edit the Internet-facing interface. Ensure that **Override internal DNS** is selected.

## Communication errors remain.

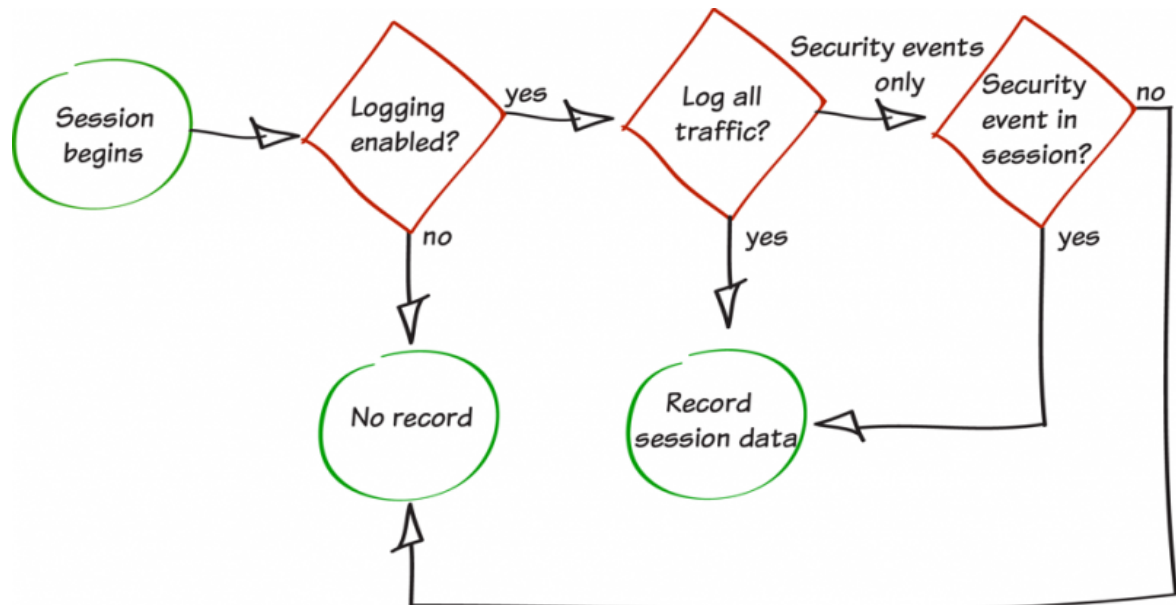
FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets.

In effort to avoid port blocking, You can configure your FortiGate unit to use higher-numbered ports, such as 2048-20000, using the following CLI command:

```
config system global
  set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use.

# Logging FortiGate traffic



In this example, you will enable logging to capture the details of the network traffic processed by your FortiGate unit. Capturing log details will provide you with detailed traffic information that you can use to asses any network issues.

A video of this recipe can be found [here](#).

## 1. Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**. Select where log messages will be recorded. You can save log messages to disk if it is supported by your FortiGate unit, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create reports based on them. In most cases, it is recommended to **Send Logs to FortiCloud**, as shown in the example.

Next, enable **Event Logging**. You can choose to Enable All types of logging, or specific types, such as WiFi activity events, depending on your needs.

Under the **GUI Preferences**, ensure that the **Display Logs From** is set to the same location where the log messages are recorded (in the example, **FortiCloud**).

The screenshot shows the 'Log Settings' configuration page. It is divided into two main sections: 'Logging and Archiving' and 'GUI Preferences'. In the 'Logging and Archiving' section, the 'Send Logs to FortiAnalyzer/FortiManager' option is unchecked, while 'Send Logs to FortiCloud' is checked. Below this, the 'Account' field is populated with 'email@example.com'. The 'Upload Option' is set to 'Realtime'. Under 'Event Logging', 'Enable All' is checked, and several specific event types are also checked: WiFi activity event, Router activity event, System activity event, VPN activity event, User activity event, and Explicit web proxy event. The 'GUI Preferences' section shows 'Display Logs From' set to 'FortiCloud'. At the bottom, there is an 'Apply' button.

| Logging and Archiving  |   |  |
|--|---|--|
| <input type="checkbox"/> Send Logs to FortiAnalyzer/FortiManager |   |  |
| IP Address:  | <input type="text"/>                                      | <button>Test Connectivity</button>                           |
| <input checked="" type="checkbox"/> Send Logs to FortiCloud      |   |  |
| Account:   | <input type="text" value="email@example.com"/>            | <button>Test Connectivity</button>                           |
| Upload Option  |   |  |
| <input checked="" type="radio"/> Realtime                        |   |  |
| <input checked="" type="checkbox"/> Event Logging                |   |  |
| <input checked="" type="checkbox"/> Enable All                   |   |  |
| <input checked="" type="checkbox"/> WiFi activity event          | <input checked="" type="checkbox"/> System activity event | <input checked="" type="checkbox"/> User activity event      |
| <input checked="" type="checkbox"/> Router activity event        | <input checked="" type="checkbox"/> VPN activity event    | <input checked="" type="checkbox"/> Explicit web proxy event |

| GUI Preferences  |   |
|--|---|
| Display Logs From  | <input type="text" value="FortiCloud"/> |
| <input checked="" type="checkbox"/> Resolve Hostnames (Using reverse DNS lookup)                     |   |
| <input checked="" type="checkbox"/> Resolve Unknown Applications (Using remote application database) |   |

Apply

## 2. Enabling logging in the security policies

Go to **Policy & Objects > Policy > IPv4**.  
Edit the policies controlling the traffic you wish to log.

Under **Logging Options**, select **All Sessions**.

In most cases, you should select Security Events, as All Sessions requires more system resources and storage space. For now, however, All Sessions will be used to verify that logging has been set up successfully.

|                     |                     |
|---------------------|---------------------|
| Destination Address | <div>all</div>      |
| Schedule            | <div>always</div>   |
| Service             | <div>ALL</div>      |
| Action              | <div>✓ ACCEPT</div> |

**Firewall / Network Options**

ON

 NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Fixed Port

Click to add...

**Security Profiles**

OFF

 AntiVirus

OFF

 Web Filter

OFF

 Application Control

OFF

 SSL Inspection

certificate-inspection

**Traffic Shaping**

OFF

 Shared Shaper

OFF

 Reverse Shaper

OFF

 Per-IP Shaper

guarantee-100kbps

guarantee-100kbps

Click to set...

**Logging Options**

ON

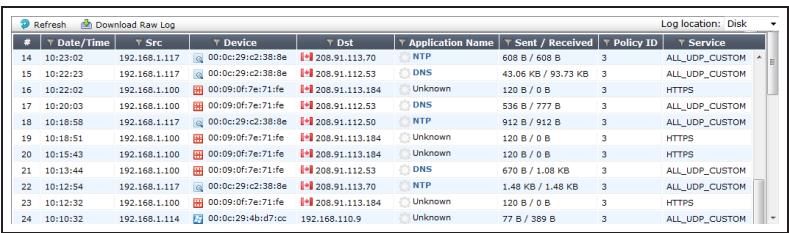
 Log Allowed Traffic

☐ Security Events

☒ All Sessions

### 3. Results

View traffic logs by going to **Log & Report > Traffic Log > Forward Traffic**. The logs display a variety of information about your traffic, including date/time, source, device, and destination. To change the information shown, right-click on any column title and select **Column Settings** to enable or disable different columns.



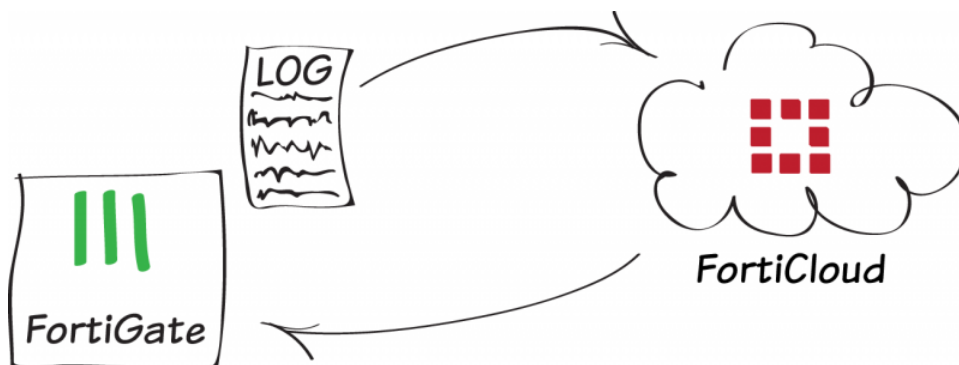
The screenshot shows the FortiOS Traffic Log interface. At the top, there are buttons for 'Refresh' and 'Download Raw Log', and a 'Log location: Disk' dropdown. The main area is a table with columns: #, Date/Time, Src, Device, Dst, Application Name, Sent / Received, Policy ID, and Service. The table contains 11 rows of log entries. Each row has a small icon to the left of the Src and Dst columns, and a status icon to the left of the Application Name column.

| #  | Date/Time | Src           | Device            | Dst            | Application Name | Sent / Received     | Policy ID | Service        |
|----|-----------|---------------|-------------------|----------------|------------------|---------------------|-----------|----------------|
| 14 | 10:23:02  | 192.168.1.117 | 00:0c:29:c2:38:8e | 208.91.113.70  | NTP              | 608 B / 608 B       | 3         | ALL_UDP_CUSTOM |
| 15 | 10:22:23  | 192.168.1.117 | 00:0c:29:c2:38:8e | 208.91.112.53  | DNS              | 43.06 KB / 93.73 KB | 3         | ALL_UDP_CUSTOM |
| 16 | 10:22:02  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.113.184 | Unknown          | 120 B / 0 B         | 3         | HTTPS          |
| 17 | 10:20:03  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.112.53  | DNS              | 536 B / 777 B       | 3         | ALL_UDP_CUSTOM |
| 18 | 10:18:58  | 192.168.1.117 | 00:0c:29:c2:38:8e | 208.91.112.50  | NTP              | 912 B / 912 B       | 3         | ALL_UDP_CUSTOM |
| 19 | 10:18:51  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.113.184 | Unknown          | 120 B / 0 B         | 3         | HTTPS          |
| 20 | 10:15:43  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.113.184 | Unknown          | 120 B / 0 B         | 3         | HTTPS          |
| 21 | 10:13:44  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.112.53  | DNS              | 670 B / 1.08 KB     | 3         | ALL_UDP_CUSTOM |
| 22 | 10:12:54  | 192.168.1.117 | 00:0c:29:c2:38:8e | 208.91.113.70  | NTP              | 1.48 KB / 1.48 KB   | 3         | ALL_UDP_CUSTOM |
| 23 | 10:12:32  | 192.168.1.100 | 00:09:0f:7e:71:fe | 208.91.113.184 | Unknown          | 120 B / 0 B         | 3         | HTTPS          |
| 24 | 10:10:32  | 192.168.1.114 | 00:0c:29:4b:d7:cc | 192.168.110.9  | Unknown          | 77 B / 389 B        | 3         | ALL_UDP_CUSTOM |

For further reading, check out [Logging and reporting overview](#) in the [FortiOS 5.2 Handbook](#).



# Logging with FortiCloud



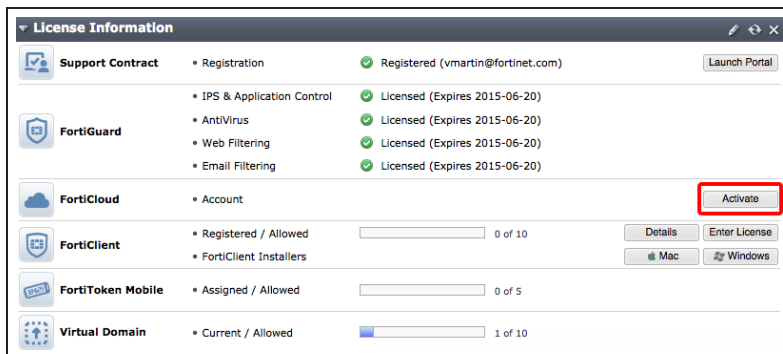
In this example, you will use FortiCloud, an online logging service provided by Fortinet, to store the logs of your FortiGate unit's traffic. You will also access logs using the [FortiCloud website](#).

*Before you can use FortiCloud, you must register your FortiGate. For more information, see [FortiGate registration and basic settings](#).*

A video of this recipe is available [here](#).

## 1. Activating FortiCloud

Go to **System > Dashboard > Status** and locate the **License Information** widget. In the **FortiCloud** section, select **Activate**.



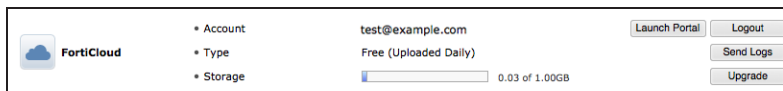
Either use an existing FortiCloud account or create a new one.

*It is recommend to use a common FortiCloud account for all your Fortinet logs.*

The 'Activate FortiCloud' dialog box contains the following fields and options:

- Action**: Radio buttons for 'Login' and 'Create Account' (selected).
- Email**: Input field with 'test@example.com'.
- Confirm Email**: Input field with 'test@example.com'.
- Password**: Input field with masked characters (dots).
- Confirm Password**: Input field with masked characters (dots).
- Agreement**: A checked checkbox 'I agree to the FortiCloud terms & conditions (View)'.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

Information about your FortiCloud account now appears in the **License Information** widget.



## 2. Sending logs to FortiCloud

Go to **Log & Report > Log Config > Log Settings**. Enable **Send Logs to FortiCloud** and ensure that **Upload Option** is set to **Realtime**.

The 'Log Settings' configuration page shows the following settings:

- Send Logs to FortiCloud**: A checked checkbox.
- Account**: Input field with 'test@example.com' and a 'Test Connectivity' button.
- Upload Option**: Radio buttons for 'Realtime' (selected) and another option.

Select **Test Connectivity** to verify the connection between your FortiGate and FortiCloud.

FortiCloud Connection Summary

Disk Quota

1024 MB

Quota Used

29 MB

DLP Archive

Close

Adjust the **Event Logging** settings as required and set the GUI Preferences to **Display Logs from FortiCloud**.

☒ Event Logging

☒ Enable All

☒ Endpoint event

☒ Router activity event

☒ WiFi activity event

☒ VPN activity event

☒ System activity event

☒ HA event

☒ User activity event

☒ Explicit web proxy event

GUI Preferences

Display Logs From

FortiCloud

☒ Resolve Hostnames (Using reverse DNS lookup)

☒ Resolve Unknown Applications (Using remote application database)

### 3. Enabling logging in your Internet access security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

ON

Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets

### 4. Results

Browse the Internet. Go to **Log & Report > Traffic Log > Forward Traffic**. In the top right corner of the screen, the **Log location** is shown as **FortiCloud**.

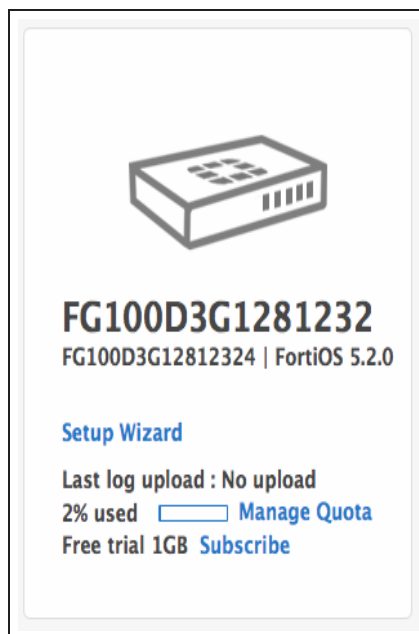
RefreshDownload Raw Log

Log location: FortiCloud

| # | Src Interface | Dst Interface | Destination                           | Action | Sent / Received    |
|---|---------------|---------------|---------------------------------------|--------|--------------------|
| 1 | port3         | wan1          | 54.225.173.54 (track.customer.io)     | close  | 2.39 KB / 6.00 KB  |
| 2 | port3         | wan1          | 54.227.237.93 (dash.generalassemb.ly) | close  | 7.54 KB / 10.82 KB |
| 3 | port3         | wan1          | 54.83.13.81 (i.kissmetrics.com)       | close  | 1.63 KB / 4.33 KB  |
| 4 | port3         | wan1          | 50.17.208.89 (trk.kissmetrics.com)    | close  | 2.62 KB / 4.67 KB  |
| 5 | port3         | wan1          | 74.125.22.95 (maps.googleapis.com)    | close  | 2.87 KB / 1.73 KB  |

Go to **System > Dashboard > Status**.  
In the **FortiCloud** section of the **License Information** widget, select **Launch Portal**. A screen will open in your browser, showing all the devices that are linked with your FortiGate account. Select the appropriate unit.

You can also access your FortiCloud account by going to [www.forticloud.com](http://www.forticloud.com)

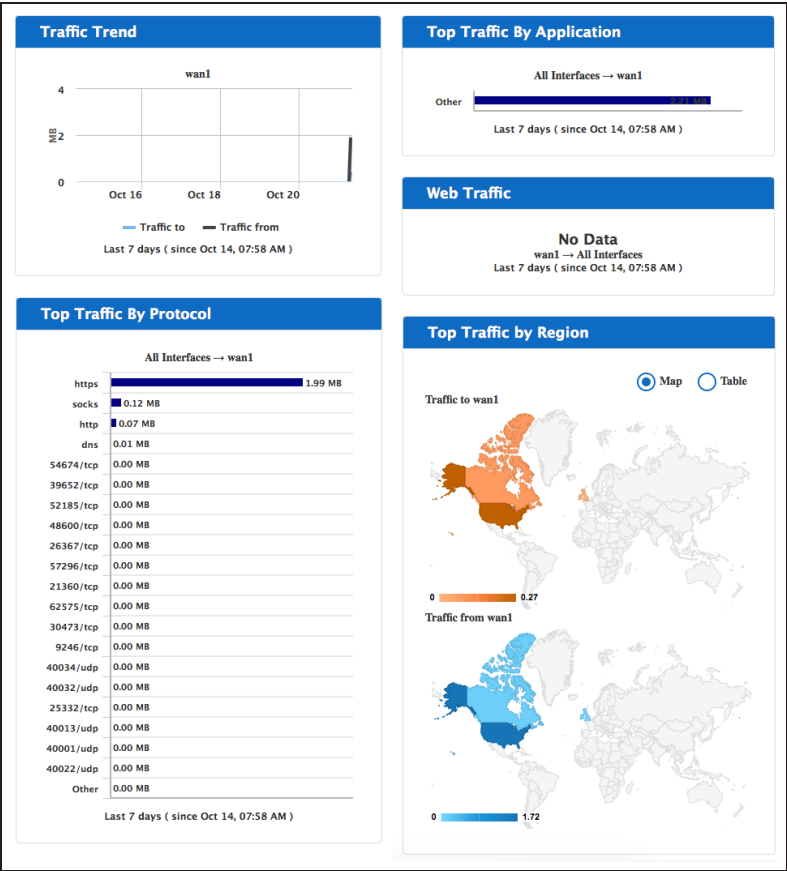


After selecting your device, the FortiCloud Dashboard appears, showing a variety of information about your traffic.

*If traffic does not appear in FortiCloud right away, wait 10-15 minutes and try again.*

From the portal, you can also access options for **FortiView**, **Drilldown**, **Reports**, and **Management**.

For more information about using FortiCloud, see the [FortiCloud FAQ](#)



For further reading, check out [FortiCloud](#) in the [FortiOS 5.2 Handbook](#).

# Troubleshooting FortiGate logging

This section contains tips to help you with some common challenges of FortiGate logging.

## No log messages appear.

Ensure that logging is enabled in both the **Log Settings** and the policy used for the traffic you wish to log, as logging will not function unless it is enabled in both places.

If logging is enabled in both places, check that the policy in which logging is enabled is the policy being used for your traffic. Also make sure that the policy is getting traffic by going to the policy list and adding the **Sessions** column to the list.

## Logs from a FortiAnalyzer, FortiManager, or from FortiCloud do not appear in the GUI.

Ensure that the correct log source has been selected in the **Log Settings**, under **GUI Preferences**.

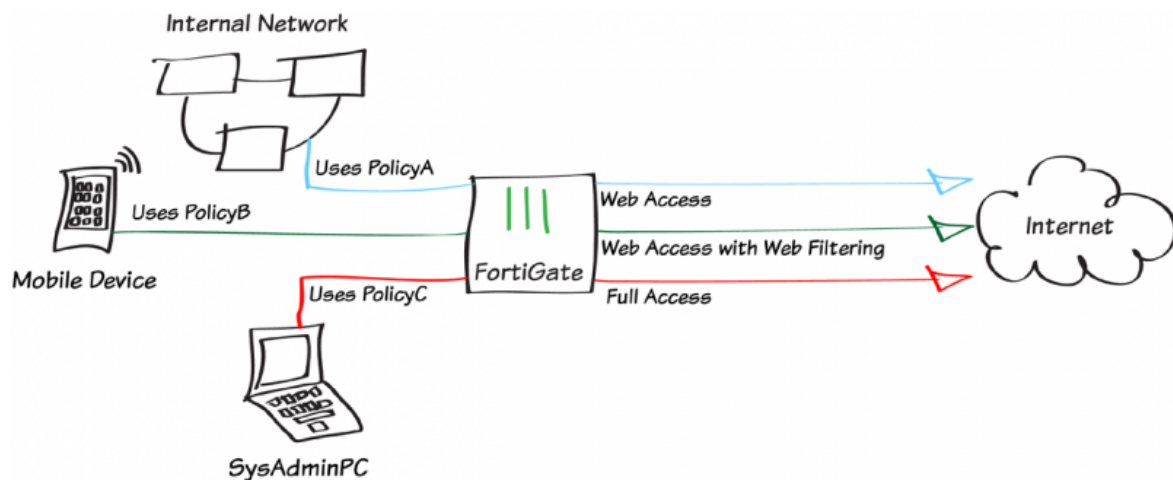
## The FortiGate unit's performance level has decreased since enabling disk logging.

If enabling disk logging has impacted overall performance, change the log settings to either send logs to a FortiAnalyzer unit, a FortiManager unit, or to FortiCloud.

## Logging to a FortiAnalyzer unit is not working as expected.

The firmware for the FortiGate and FortiAnalyzer units may not be compatible. Check the firmware release notes, found at [support.fortinet.com](https://support.fortinet.com), to see if this is the case.

# Creating security policies



This example shows how to create and order multiple security policies in the policy table, in order to apply the appropriate policy to various types of network traffic.

In the example, three IPv4 policies will be configured. PolicyA will be a general policy allowing Internet access to the LAN. PolicyB will allow Internet access while applying web filtering for specific mobile devices connecting through the LAN. PolicyC will allow the system administrator's PC (named SysAdminPC) to have full access

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, see [Setting up a WiFi bridge with a FortiAP](#).

A fourth policy, the default “deny” policy, will also be used.

A video of this recipe can be found [here](#).

# 1. Configuring PolicyA to allow general web access

Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing outgoing traffic.

Set **Service** to **HTTP**, **HTTPS**, and **DNS**.

Ensure that you have enabled **NAT**.

Incoming Interface

lan

+

Source Address

all

+

Source User(s)

Click to add...

Source Group(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

+

Destination Address

all

+

Schedule

always

Service

HTTP

X

+

HTTPS

X

DNS

X

Action

ACCEPT

+

Firewall / Network Options

ON

NAT

Use Destination Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

Use Central NAT Table

OFF

Web Cache

OFF

WAN Optimization

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

ON

Log Allowed Traffic

Security Events

All Sessions

Capture Packets



## 2. Creating PolicyB to allow access for mobile devices

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to **lan**, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones).

*Using a device group will automatically enable device identification on the lan interface.*

**Outgoing Interface** to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.

Enable **NAT**.

Under **Security Profiles**, enable **Web Filter** and set it to use the **default** profile. This action will enable **Proxy Options** and **SSL Inspection**. Use the **default** profile for **Proxy Options** and set **SSL Inspection** to **certificate-inspection** to allow HTTPS traffic to be inspected.

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Incoming Interface: lan  
Source Address: all  
Source User(s): Click to add...  
Source Group(s): Click to add...  
Source Device Type: Mobile Devices  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: always  
Service: HTTP, HTTPS, DNS  
Action: ACCEPT

**Firewall / Network Options**

☒ NAT

☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool  
☐ Use Central NAT Table

☐ Web Cache  
☐ WAN Optimization  
☐ Compliant with FortiClient Profile

**Security Profiles**

☐ AntiVirus: default  
☒ Web Filter: default  
☐ Application Control: default  
☐ IPS: default  
☐ Email Filter: default  
☐ DLP Sensor: default  
☐ VoIP: default  
☐ ICAP: default  
Proxy Options: default  
☒ SSL/SSH Inspection: default

**Logging Options**

☒ Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets

### 3. Defining SysAdminPC

Go to **User & Device > Device > Device Definitions** and create a new definition for the system administrator's PC.

Select an appropriate **Alias**, then set the **MAC Address**. Set the appropriate **Device Type**.

|                 |  |
|-----------------|--|
| Alias           | <input type="text" value="SysAdminPC"/>        |
| MAC Address     | <input type="text" value="c4:2c:03:21:af:04"/> |
| Additional MACs | <input type="text" value="Click to add..."/>   |
| Device Type     | <input type="text" value="Mac"/>               |

### 4. Configuring PolicyC to allow access for SysAdminPC

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to **lan**, **Source Device Type** to SysAdminPC, **Outgoing Interface** to your Internet-facing interface, and **Service** to **ALL**.

Enable NAT.

|                     |  |
|---------------------|--|
| Incoming Interface  | <input type="text" value="lan"/>             |
| Source Address      | <input type="text" value="all"/>             |
| Source User(s)      | <input type="text" value="Click to add..."/> |
| Source Group(s)     | <input type="text" value="Click to add..."/> |
| Source Device Type  | <input type="text" value="SysAdminPC"/>      |
| Outgoing Interface  | <input type="text" value="wan1"/>            |
| Destination Address | <input type="text" value="all"/>             |
| Schedule            | <input type="text" value="always"/>          |
| Service             | <input type="text" value="ALL"/>             |
| Action              | <input type="text" value="ACCEPT"/>          |

**Firewall / Network Options**

☒ NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

**Logging Options**

☒ Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets

## 5. Ordering the policy table

Go to **Policy & Objects > Policy > IPv4** to view the policy table. Currently, the policies are arranged in the order they were created: PolicyA is at the top, followed by PolicyB, PolicyC, and the default deny policy.

In order to have the correct traffic flowing through each policy, they must be arranged so that the more specific policies are located at the top.

*In the example, the policy table has been set to show only the columns that best display the differences between the policies. To do this, right-click on the top of the table, select or deselect columns as necessary, then select **Apply**.*

To rearrange the policies, select the column on the far left (in the example, **Seq.#**) and drag the policy to the desired position.

| Seq.# | From | To   | Service              | Web Filter  | Devices        |
|-------|------|------|----------------------|-------------|----------------|
| 1     | lan  | wan1 | HTTP<br>HTTPS<br>DNS |             |                |
| 2     | lan  | wan1 | HTTP<br>HTTPS<br>DNS | WEB default | Mobile Devices |
| 3     | lan  | wan1 | ALL                  |             | SysAdminPC     |
| 4     | any  | any  | ALL                  |             |                |

| Seq.# | From | To   | Service              | Web Filter  | Devices        |
|-------|------|------|----------------------|-------------|----------------|
| 1     | lan  | wan1 | ALL                  |             | SysAdminPC     |
| 2     | lan  | wan1 | HTTP<br>HTTPS<br>DNS | WEB default | Mobile Devices |
| 3     | lan  | wan1 | HTTP<br>HTTPS<br>DNS |             |                |
| 4     | any  | any  | ALL                  |             |                |

## 6. Results

Browse the Internet using the system administrator's PC, a different PC, and a mobile device.

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic from the three devices flows through different policies. In the example, the SysAdmin PC (IP 10.10.11.10), a Windows PC (IP 10.10.11.14), and an iPad (IP 10.10.11.13) were used to generate traffic.

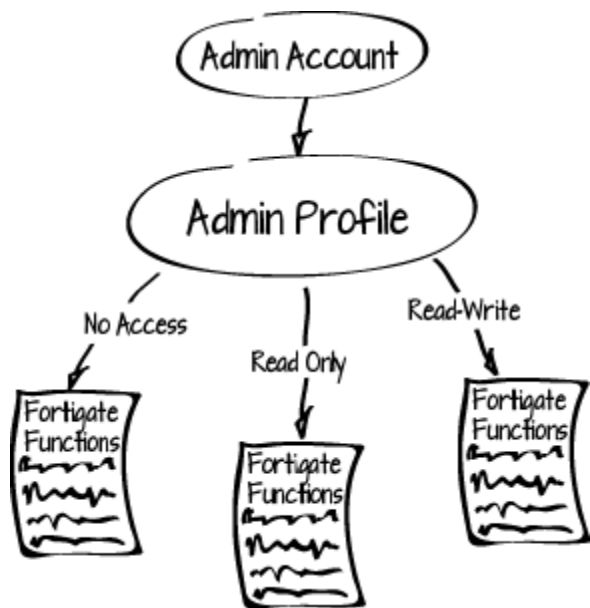
*Policy ID is automatically assigned to a policy when it is created, and so, in the example, the ID for PolicyA is 1, PolicyB is 2, and PolicyC is 3.*

| #  | Policy ID | Date/Ti... | Source      | Destination                                     | Device            |
|----|-----------|------------|-------------|---|-------------------|
| 1  | 3         | 13:42:18   | 10.10.11.10 | 72.167.239.239 (ocsp.godaddy.com.akadns.net)    | SysAdminPC        |
| 2  | 3         | 13:42:18   | 10.10.11.10 | 208.91.114.193                                  | SysAdminPC        |
| 3  | 3         | 13:42:18   | 10.10.11.10 | 192.0.65.242 (poll daddy.com)                   | SysAdminPC        |
| 4  | 3         | 13:42:18   | 10.10.11.10 | 208.91.114.193                                  | SysAdminPC        |
| 5  | 3         | 13:42:18   | 10.10.11.10 | 192.0.65.242 (poll daddy.com)                   | SysAdminPC        |
| 6  | 3         | 13:42:18   | 10.10.11.10 | 208.91.114.193                                  | SysAdminPC        |
| 7  | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 8  | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 9  | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 10 | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 11 | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 12 | 1         | 13:41:55   | 10.10.11.14 | 74.125.226.133 (safebrowsing-cache.google.com)  | 00:26:22:6c:be:d6 |
| 13 | 2         | 13:39:51   | 10.10.11.13 | 17.134.126.129 (gs-loc.ls-apple.com.akadns.net) | d8:a2:5e:1d:b1:a6 |
| 14 | 2         | 13:39:34   | 10.10.11.13 | 66.235.138.194 (metrics.apple.com)              | d8:a2:5e:1d:b1:a6 |
| 15 | 2         | 13:39:34   | 10.10.11.13 | 184.87.13.15 (e3191.dscc.akamaiedge.net)        | d8:a2:5e:1d:b1:a6 |
| 16 | 2         | 13:39:34   | 10.10.11.13 | 23.0.160.208 (images.apple.com)                 | d8:a2:5e:1d:b1:a6 |

(Optional) Attempt to make an SSL connection to a web server with all three devices. Only the system administrator's PC will be able to connect.

For further reading, check out **Firewall policies** in the **FortiOS 5.2 Handbook**.

# Limited access administrator accounts



In this recipe you will create a FortiGate administrator account that is limited to read and write access for user and device authentication and read access for logging and reporting. In addition you will use the Trusted Hosts feature to control the IP address that the administrator can log in from.

*The administrator account will have the same access limitations for both the GUI and CLI.*

# 1. Creating a new administrator profile

Go to **System > Admin > Admin Profiles**.

Create a new administrator profile that limits administrators with this profile to read and write access to **User and Devices** and read only access to **Log & Report** data and report access.

Profile Name:

User-Device-Config

Comments:

Admin account that can edit and view user and device settings and view log messages and reports95/255

Access Control

☐ None☐ Read Only☐ Read-Write



|                                |                                  |                                  |                                  |
|--------------------------------|----------------------------------|----------------------------------|----------------------------------|
| System Configuration           | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Network Configuration          | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Administrator Users            | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| FortiGuard Update              | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Maintenance                    | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Router Configuration           | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Firewall Configuration         | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Security Profile Configuration | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| VPN Configuration              | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| User & Device                  | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| WAN Opt & Cache                | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Endpoint Security              | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| WiFi Controller                | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Log & Report                   | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            |
| Configuration                  | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| Data Access                    | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            |
| Report Access                  | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            |
| Threat Weight                  | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |

## 2. Adding a new administrator and assigning the profile

Go to **System > Admin > Administrators**.

Create a new administrator account and assign it to the **Administrator Profile** that you just created.

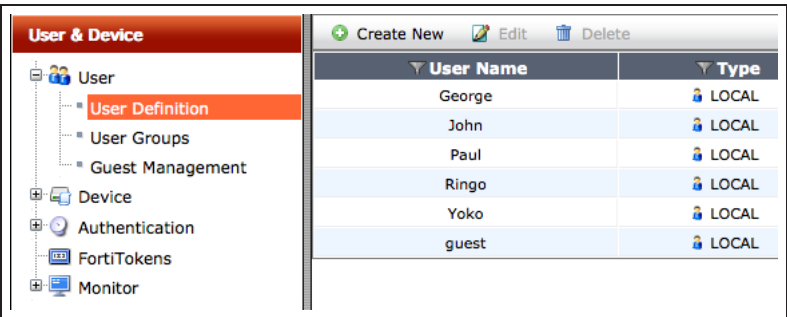
Add an IP address to at least one of the **Trusted Host** fields to control where the administrator can log in from. In the example the administrator can log in only from the 172.20.120.0 network.

|   |   |
|---|---|
| Administrator   | <input type="text" value="t.white"/>  |
| Type  | <input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI                                     |
| Password  | <input type="password" value="....."/>  |
| Confirm Password  | <input type="password" value="....."/>  |
| Comments  | <input type="text" value="User and device admin account"/> 29/255   |
| Administrator Profile   | <input type="text" value="User-Device-Config"/>  |
| Contact Info  |   |
| <input checked="" type="checkbox"/> Email Address   | <input type="text" value="t.white@example.com"/>  |
| <input type="checkbox"/> SMS  | <input checked="" type="radio"/> FortiGuard Messaging Service <input type="radio"/> Custom  |
|   | Country/Region <input type="text" value="Click to add..."/>   |
|   | Phone Number <input type="text"/>   |
| <input type="checkbox"/> Enable Two-factor Authentication                                     |   |
| <input checked="" type="checkbox"/> Restrict this Administrator Login from Trusted Hosts Only |   |
| Trusted Host #1   | <input type="text" value="172.20.120.0/24"/>  |
| Trusted Host #2   | <input type="text" value="0.0.0.0/0.0.0.0"/>  |
| Trusted Host #3   | <input type="text" value="0.0.0.0/0.0.0.0"/>     |

### 3. Results

Log into the FortiGate unit with the t.white. administrator account. t.white should only see the **User & Device** and the **Log & Report** menus.

t.white should be able to change user and device authentication settings and view log messages and reports.

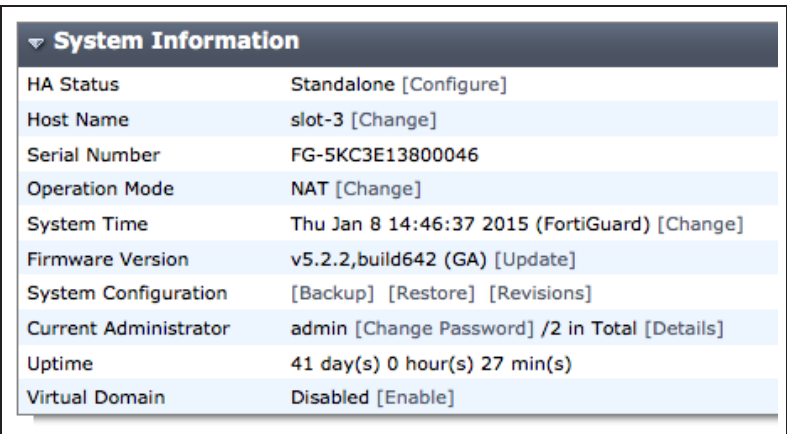


| User & Device          |       |
|------------------------|-------|
| Create New Edit Delete |       |
| User Name              | Type  |
| George                 | LOCAL |
| John                   | LOCAL |
| Paul                   | LOCAL |
| Ringo                  | LOCAL |
| Yoko                   | LOCAL |
| guest                  | LOCAL |

Log in from another browser window with the admin account.

Go to **System > Dashboard > Status**, and view the **System Information** widget. It should show two administrators.

Select **Details** to view the list of logged in administrators.



| System Information    |   |
|-----------------------|---|
| HA Status             | Standalone [Configure]                        |
| Host Name             | slot-3 [Change]                               |
| Serial Number         | FG-5KC3E13800046                              |
| Operation Mode        | NAT [Change]                                  |
| System Time           | Thu Jan 8 14:46:37 2015 (FortiGuard) [Change] |
| Firmware Version      | v5.2.2,build642 (GA) [Update]                 |
| System Configuration  | [Backup] [Restore] [Revisions]                |
| Current Administrator | admin [Change Password] /2 in Total [Details] |
| Uptime                | 41 day(s) 0 hour(s) 27 min(s)                 |
| Virtual Domain        | Disabled [Enable]                             |



| Administrators logged in         |                    |       |                |                         |
|----------------------------------|--------------------|-------|----------------|-------------------------|
| Disconnect Refresh               |                    |       |                |                         |
| User Name                        | Access Profile     | Type  | From           | Time                    |
| <input type="checkbox"/> t.white | User-Device-Config | https | 172.20.120.223 | Thu Jan 8 14:41:46 2015 |
| <input type="checkbox"/> admin   | super_admin        | https | 172.20.120.223 | Thu Jan 8 14:46:36 2015 |



Using the admin or t.white account, go to **Log & Report > Event Log > System**.

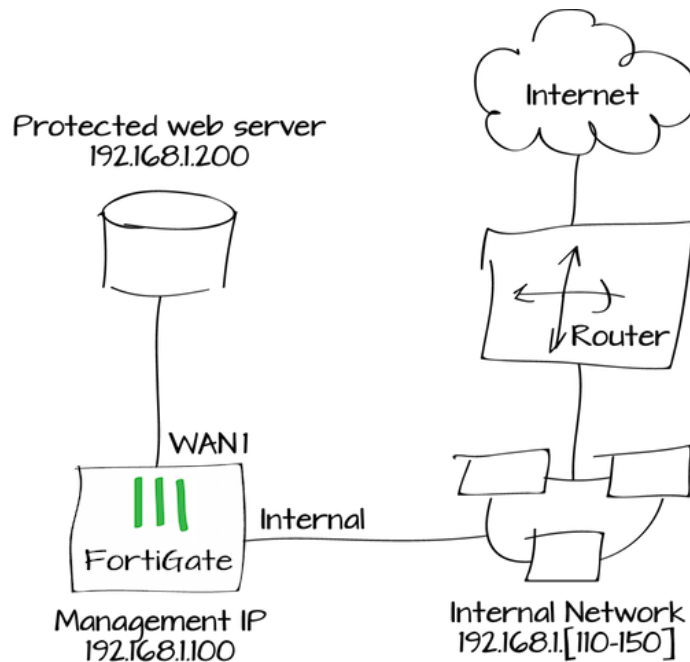
Log messages should show activity for both administrators. Select a log entry to view details. Log entries for t.white should show the source address that t.white logged in from. This address should be within the Trusted Hosts network address.

| # | Date/Time | Level   | User    | Message   |
|---|-----------|---------|---------|---|
| 3 | 14:51:50  | Success | t.white | Administrator t.white logged in successfully from https(172.20.120.223) |
| 4 | 14:51:44  | Success | admin   | Administrator admin logged out from https(172.20.120.223)               |
| 5 | 14:51:34  | Success | admin   | Administrator admin logged in successfully from https(172.20.120.223)   |
| 6 | 14:51:23  | Success | t.white | Configuration is changed in the admin session                           |
| 7 | 14:51:23  | Success | t.white | Administrator t.white timed out on https(172.20.120.223)                |

|                 |   |                |                       |
|-----------------|---|----------------|-----------------------|
| #               | 1   | Action         | login                 |
| Date/Time       | 14:57:11  | Level          | Success               |
| Log Description | Admin logged in successfully  | Log ID         | 32001                 |
| Message         | Administrator t.white logged in successfully from https(172.20.120.223) | Profile Name   | User-Device-Config    |
| Reason          | none  | Status         | success               |
| Sub Type        | system  | Timestamp      | 1/8/2015, 2:57:11 PM  |
| User            | t.white   | User Interface | https(172.20.120.223) |
| Virtual Domain  | root  |                |                       |

For further reading, check out [Administrators](#) in the [FortiOS 5.2 Handbook](#).

# Port pairing in Transparent mode



When you create a port pair, all traffic accepted by one of the paired interfaces can only exit out the other interface. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

In this example you will create a wan1 to Internal port pair to make it easier to allow access to a web server protected by a FortiGate in Transparent mode. In this unusual configuration, the web server is connected to the FortiGate's wan1 interface and the FortiGate's Internal interface is connected to an internal network. Users on the internal network access the web server through the FortiGate.

Traffic between port-paired interfaces does not check the bridge table and MAC addresses are not learned. Instead traffic received by one interface in a port pair is forwarded out the other (if allowed by a firewall policy). This makes port pairing useful for unusual topologies where MAC addresses do not behave normally. For example, port pairing can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

## 1. Switching the FortiGate unit to transparent mode and adding a static route

Go to **System > Dashboard > Status**.

In the **System Information** widget, select **Change** beside **Operation Mode**.

Change the **Operation Mode** to **Transparent**. Add a **Management IP/Netmask**. Also add a **Default Gateway** for your network so that the FortiGate unit can connect to the Internet.

*If the Management IP is the same as the IP address that you logged into the FortiGate unit with, you will remain logged in after the operation mode has changed. Otherwise, log into the FortiGate unit using the management IP (in the example, 172.20.120.142).*

|                       |                  |
|-----------------------|------------------|
| Operation Mode        | Transparent      |
| Management IP/Netmask | 192.168.1.100/24 |
| Default Gateway       | 192.168.1.2      |

## 2. Creating an internal and wan1 port pair

Go to **System > Network > Interfaces**.

Select **Create New > Port Pair**. Create a port pair that includes the internal and wan1 interfaces.

All traffic accepted by the internal interface can only exit out of the wan1 interface.

|   |                              |
|---|------------------------------|
| Name: Internal-wan1-port-pair   |                              |
| Available Members:  | Selected Members(must be 2): |
| port12<br>port13<br>port14<br>port15<br>port16<br>port2<br>port3<br>port4<br>port5<br>port6<br>port7<br>port8 | Internal<br>wan1             |

### 3. Creating security policies

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy that allows internal users to access the protected web server using HTTP and HTTPS.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | Internal        |
| Source Address      | all             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address | Web-Server      |
| Schedule            | always          |
| Service             | HTTP<br>HTTPS   |
| Action              | ACCEPT          |

Create a second security policy that allows connections from the web server to the internal network and to the Internet using any service.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | wan1            |
| Source Address      | Web-Server      |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | Internal        |
| Destination Address | all             |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

### 4. Results

Connect to the web server from the internal network and surf the Internet from the server itself.

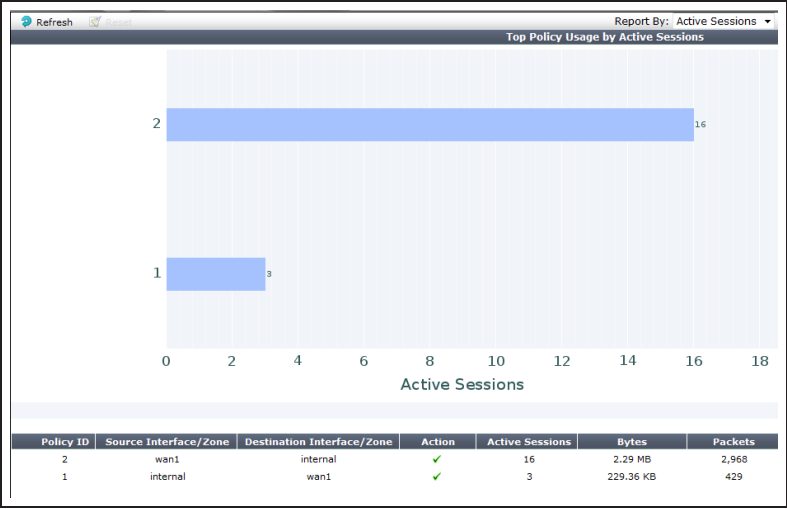
Go to **Log & Report > Traffic Log > Forward Traffic** to verify that there is traffic from the internal to wan1 interface.

Select an entry for details.

| #  | Date/Time | Src Interface | Dst Interface | Src           | Dst            | Sent / Received    | Policy ID | Service  |
|----|-----------|---------------|---------------|---------------|----------------|--------------------|-----------|----------|
| 1  | 11:05:11  | wan1          | internal      | 192.168.1.200 | 8.8.8.8        | 75 B / 277 B       | 2         | DNS      |
| 2  | 11:05:11  | wan1          | internal      | 192.168.1.200 | 74.125.225.223 | 1.04 KB / 9.08 KB  | 2         | HTTPS    |
| 3  | 11:05:06  | wan1          | internal      | 192.168.1.200 | 74.125.226.79  | 728 B / 2.62 KB    | 2         | HTTPS    |
| 4  | 11:05:02  | wan1          | internal      | 192.168.1.200 | 192.168.1.99   | 0 B / 1.72 KB      | 2         | 8010/tcp |
| 5  | 11:04:46  | internal      | wan1          | 192.168.1.111 | 192.168.1.200  | 164 B / 132 B      | 1         | HTTP     |
| 6  | 11:04:46  | internal      | wan1          | 192.168.1.111 | 192.168.1.200  | 164 B / 132 B      | 1         | HTTP     |
| 7  | 11:04:42  | wan1          | internal      | 192.168.1.200 | 192.168.1.99   | 0 B / 1.72 KB      | 2         | 8010/tcp |
| 8  | 11:04:27  | internal      | wan1          | 192.168.1.111 | 192.168.1.200  | 1.46 KB / 2.92 KB  | 1         | HTTPS    |
| 9  | 11:04:27  | internal      | wan1          | 192.168.1.111 | 192.168.1.200  | 1.33 KB / 2.70 KB  | 1         | HTTPS    |
| 10 | 11:04:27  | internal      | wan1          | 192.168.1.111 | 192.168.1.200  | 1.33 KB / 2.75 KB  | 1         | HTTPS    |
| 11 | 11:04:22  | wan1          | internal      | 192.168.1.200 | 192.168.1.99   | 0 B / 1.72 KB      | 2         | 8010/tcp |
| 12 | 11:04:21  | wan1          | internal      | 192.168.1.200 | 74.125.226.67  | 58.96 KB / 2.06 MB | 2         | HTTP     |

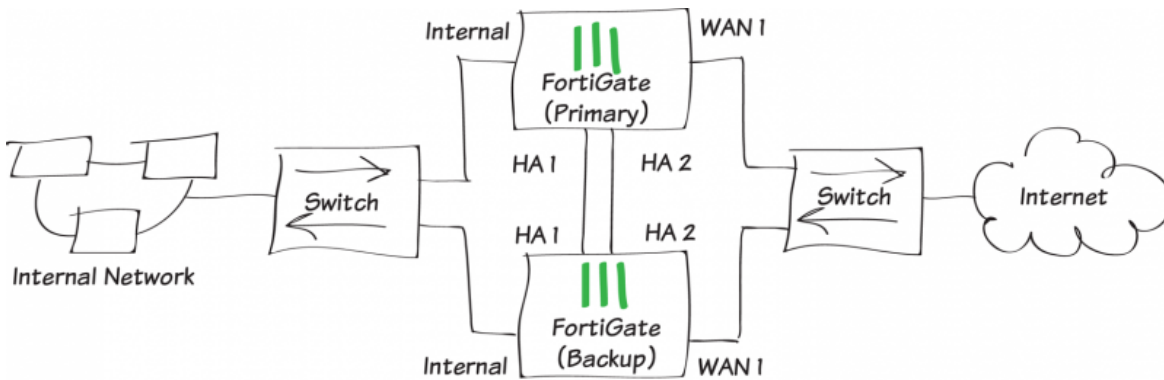
|                          |                                     |                            |                   |
|--------------------------|-------------------------------------|----------------------------|-------------------|
| Dst                      | 74.125.225.223                      | Virtual Domain             | root              |
| Received                 | 9296                                | Source Country             | Reserved          |
| Application Name         | SSL                                 | Sent / Received            | 1.04 KB / 9.08 KB |
| Duration                 | 17                                  | Sent                       | 1067              |
| Application Details      |                                     | Service                    | HTTPS             |
| Protocol                 | 6                                   | Destination Country        | United States     |
| Application Control List | default                             | Dst Port                   | 443               |
| roll                     | 65531                               | Status                     | close             |
| Timestamp                | Wed Mar 13 11:05:11 2013            | Tran Display               | noop              |
| Sequence Number          | 700150                              | Policy ID                  | 2                 |
| Src Interface            | wan1                                | Src                        | 192.168.1.200     |
| Sent Packets             | 15                                  | Level                      | notice            |
| Application Category     | Web.Surfing                         | Application ID             | 15895             |
| Src Port                 | 51218                               | Application Control Action | detected          |
| Log ID                   | 13                                  | Sub Type                   | forward           |
| Threat                   |                                     | Received Packets           | 13                |
| Date/Time                | 11:05:11 (Wed Mar 13 11:05:11 2013) | Dst Interface              | internal          |

Go to **Policy & Objects > Monitor > Policy Monitor** to view the active sessions.



For further reading, check out **Interfaces** in the **FortiOS 5.2 Handbook**.

# How to upgrade one unit in an HA cluster



In this recipe, which starts with a FortiGate Clustering Protocol (FGCP) cluster of two FortiGate units\*, you will upgrade the primary unit's firmware, while keeping the subordinate unit as a failsafe backup running the original firmware.

If the new firmware upgrades and runs successfully, you can quickly upgrade the entire cluster to the new firmware. If the new firmware fails during or after the upgrade, you can quickly revert the cluster to the older firmware.

This recipe increases the effort needed to upgrade cluster firmware but allows easily falling back to the original firmware version and FortiGate configuration with minimal network interruption.

Normally when you upgrade a cluster, network traffic is not interrupted. However, upgrading one unit in a cluster results in minor network disruptions similar to upgrading the firmware of a single FortiGate unit.

This recipe requires you to enable the dedicated or reserved HA management interface feature.

This example uses the following interfaces:

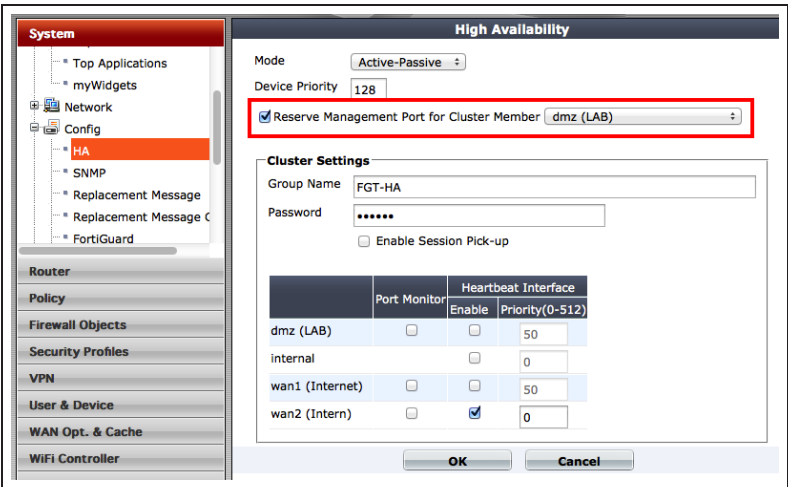
- Internal1 is the reserved management interface
- Internal2 is connected to the Internal Network
- wan1 is connected to the Internet
- Internal4 and Internal5 are the HA heartbeat interfaces

# 1. Enable the HA reserved management interface feature

You can configure the HA reserved management interface feature when originally setting up the cluster.

If the cluster is already running, log into the primary unit and go to **System > Config > HA**, select the primary unit, enable the reserved management interface, and select an interface.

Then go to **System > Network > Interface** and configure the interface that you selected.



You can also use the following command to set up the reserved management interface from the CLI. This is also the only way to add a default gateway for the reserved management interface if one is required.

```
config system ha
    set ha-mgmt-interface internal1
    set ha-mgmt-interface-gateway 10.11.101.2
end
```

set ha-mgmt-interface-gateway 10.11.101.2

To configure the subordinate unit's reserved management interface, from the primary unit CLI use the `execute ha manage` command to access the subordinate unit's CLI. Then use the `config system interface` command to set the IP address for the subordinate unit reserved management interface. You can also use the `set ha-mgmt-interface-gateway` command to configure the default gateway.

Enabling and selecting the reserved management interface is synchronized to both cluster members. The management interface gateway and the configuration of the management interface is not synchronized.

## 2. Disable HA configuration synchronization

Enter this command to disable HA configuration synchronization. You can enter this command from any CLI prompt on the primary unit (master) or subordinate unit (slave). The change is synchronized to both FortiGate units in the cluster.

```
config system ha
set sync-config disable
end
```

## 3. Back up the configuration of each cluster unit

Use the reserved management IP addresses to log into the GUI of each cluster unit and verify that the serial numbers and role of the unit in the cluster match. The first image shows an example primary unit (master) and the second an example subordinate unit (slave).

Primary unit (master)

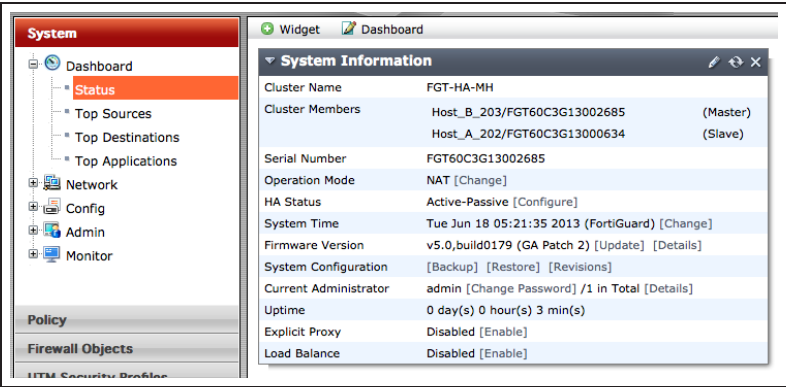
| System Information    |   |
|-----------------------|---|
| Cluster Name          | FGT-HA-MH   |
| Cluster Members       | Host_B_203/FGT60C3G13002685 (Master)<br>Host_A_202/FGT60C3G13000634 (Slave) |
| Serial Number         | FGT60C3G13002685  |
| Operation Mode        | NAT [Change]  |
| HA Status             | Active-Passive [Configure]  |
| System Time           | Tue Jun 18 05:21:35 2013 (FortiGuard) [Change]                              |
| Firmware Version      | v5.0,build0179 (GA Patch 2) [Update] [Details]                              |
| System Configuration  | [Backup] [Restore] [Revisions]  |
| Current Administrator | admin [Change Password] /1 in Total [Details]                               |
| Uptime                | 0 day(s) 0 hour(s) 3 min(s)   |
| Explicit Proxy        | Disabled [Enable]   |
| Load Balance          | Disabled [Enable]   |

Subordinate unit (slave)

| System Information    |   |
|-----------------------|---|
| Cluster Name          | FGT-HA-MH   |
| Cluster Members       | Host_A_202/FGT60C3G13000634 (Slave)<br>Host_B_203/FGT60C3G13002685 (Master) |
| Serial Number         | FGT60C3G13000634  |
| Operation Mode        | NAT [Change]  |
| HA Status             | Active-Passive [Configure]  |
| System Time           | Tue Jun 18 15:57:07 2013 (FortiGuard) [Change]                              |
| Firmware Version      | v5.0,build0208 (GA Patch 3) [Update] [Details]                              |
| System Configuration  | [Backup] [Restore] [Revisions]  |
| Current Administrator | admin [Change Password] /1 in Total [Details]                               |
| Uptime                | 0 day(s) 9 hour(s) 1 min(s)   |

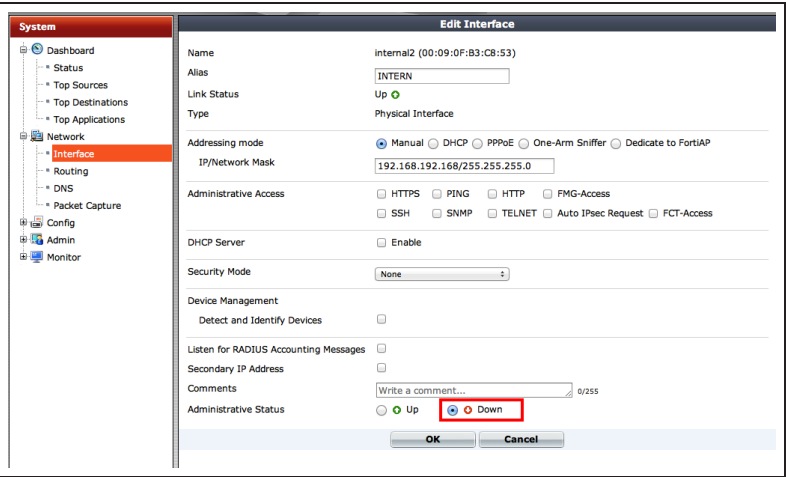


From the system information dashboard widget of each cluster unit GUI, back up each cluster unit's configuration. Back up both configurations since some settings are not synchronized (for example, the reserved management IP address).

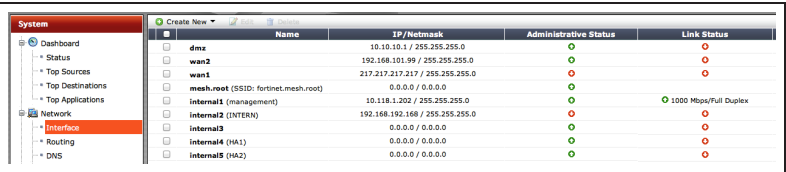


#### 4. Isolate the subordinate unit

Isolate of the subordinate unit from the network. From the subordinate unit GUI, go to **System > Network > Interface**, edit the traffic interfaces (in this example *Internal2* and *wan1*) and set their **Administrative Status** to **Down**.

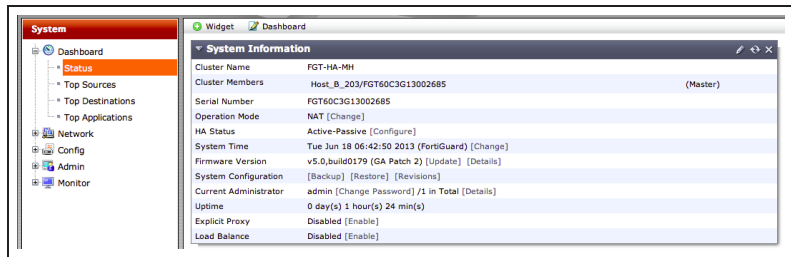


Isolate of the subordinate unit from the primary unit. Set the **Administrative Status** of the heartbeat interfaces (*Internal4* and *Internal5*) to **Down**.

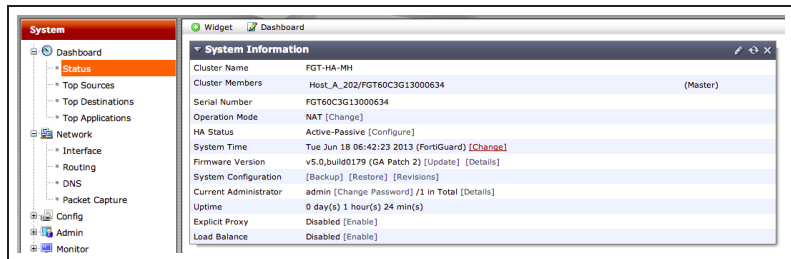


To avoid a split brain (when the heartbeat interfaces become disconnected and both cluster members become primary units) you must bring the traffic interfaces down before the heartbeat interfaces.

Check the **System Information** widget of the subordinate unit. It will think its the primary unit. Because its traffic interfaces are down, all traffic is going to the actual primary unit.



Connect to the primary unit GUI. The **System Information** widget should show just one cluster member.



## 5. Upgrade the cluster firmware and re-establish the cluster

Upgrade the firmware running on the primary unit (the one still processing traffic) using any normal firmware update procedure. For a short time during the upgrade network traffic is blocked. After the upgrade, make sure the primary unit is operating as expected. If it is not, go to step 6. **Revert to the original firmware version.**

Once you have done enough testing to establish that the primary unit is operating as expected with the new firmware, you can upgrade the subordinate unit to the same version. Log into the subordinate unit using its reserved management interface and upgrade the firmware.

Log into the primary unit reserved management interface and re-enable configuration synchronization.

```
config system ha
set sync-config enable
end
```

Log into the subordinate unit, enable configuration synchronization, bring up its heartbeat interfaces and bring up its traffic interfaces.

The cluster resumes operating normally. You can use the `get system ha status` and `diagnose sys ha status` commands to verify that HA is operating normally.

Back up the configuration of the primary and subordinate FortiGate units. Backed up configuration files are specific to FortiOS versions.

## 6. Revert to the original firmware version

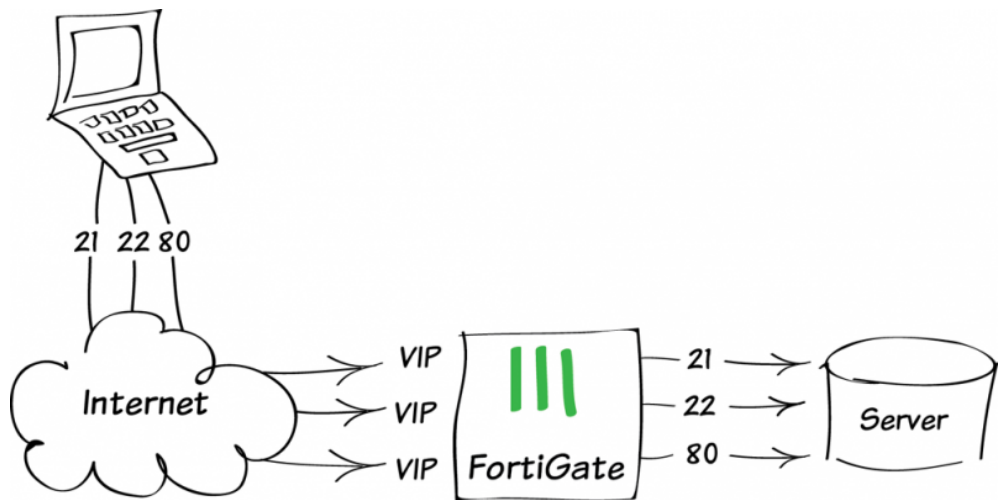
If the update didn't succeed or the primary unit is not operating as expected, bring down the primary unit traffic interfaces and then heartbeat interfaces.

Then bring up the subordinate unit traffic and heartbeat interfaces. The subordinate unit, running the original firmware version, becomes the primary unit and processes traffic normally.

Downgrade the firmware running on the original primary unit to the original firmware version (that is currently running on the subordinate unit). Bring up the heartbeat and traffic interfaces on the original primary unit. The two cluster members re-establish the cluster, running the original firmware version.

For further reading, check out [Configuring and connecting HA clusters](#) in the [FortiOS 5.2 Handbook](#).

# Port forwarding



This example illustrates how to use virtual IPs to configure port forwarding on a FortiGate unit. In this example, TCP ports 80 (HTTP), 21 (FTP), and 22 (SSH) are opened, allowing remote connections to communicate with a server behind the firewall.

A video of this recipe can be found [here](#).

## 1. Creating three virtual IPs

Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP**.

Enable **Port Forwarding** and add a virtual IP for TCP port 80. Label this VIP *webserver-80*.

*While this example maps port 80 to port 80, any valid External Service port can be mapped to any listening port on the destination computer.*

The screenshot shows the configuration for a new Virtual IP named 'webserver-80'. The 'VIP Type' is set to 'IPv4 VIP'. The 'Interface' is 'wan2'. The 'Type' is 'Static NAT'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'TCP'. The 'External Service Port' is 80, and the 'Map to Port' is also 80. The 'Mapped IP Address/Range' is 192.168.111.99. The 'External IP Address/Range' is left blank. The 'Source Address Filter' checkbox is unchecked. The 'Comments' field is empty.

Create a second virtual IP for TCP port 22. Label this VIP *webserver-ssh*.

The screenshot shows the configuration for a new Virtual IP named 'webserver-ssh'. The 'VIP Type' is set to 'IPv4 VIP'. The 'Interface' is 'Any'. The 'Type' is 'Static NAT'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'TCP'. The 'External Service Port' is 22, and the 'Map to Port' is also 22. The 'Mapped IP Address/Range' is 192.168.111.99. The 'External IP Address/Range' is left blank. The 'Source Address Filter' checkbox is unchecked. The 'Comments' field is empty.

Create a third a virtual IP for TCP port 21.  
Label this VIP *webserver-ftp*.

VIP Type

☒ IPv4 VIP ☐ IPv6 VIP ☐ NAT46 VIP ☐ NAT64 VIP

Name

webserver-ftp

Comments

Write a comment... 0/255

Interface

wan2

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

Mapped IP Address/Range

192.168.111.99 - 192.168.111.99

☒ Port Forwarding

Protocol

☒ TCP ☐ UDP ☐ SCTP

External Service Port

21 - 21

Map to Port

21 - 21

## 2. Adding virtual IPs to a VIP group

Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP Group**.

Create a VIP group. Under **Members**, include all three virtual IPs previously created.

Type

☒ IPv4 VIP Group ☐ IPv6 VIP Group ☐ NAT46 VIP Group ☐ NAT64 VIP Group

Name

Webserver

Comments

Write a comment... 0/255

Interface

wan2

Members

webserver-80

webserver-ftp

webserver-ssh

### 3. Creating a security policy

Go to **Policy & Objects > Policy > IPv4** and create a security policy allowing access to a server behind the firewall.

Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination Address** to the VIP group. Set **Service** to allow **HTTP**, **FTP**, and **SSH** traffic.

Use the appropriate **Security Profiles** to protect the servers.

|                     |                 |     |
|---------------------|-----------------|-----|
| Incoming Interface  | wan2            | +   |
| Source Address      | all             | +   |
| Source User(s)      | Click to add... |     |
| Source Device Type  | Click to add... |     |
| Outgoing Interface  | internal1       | +   |
| Destination Address | Webserver       | +   |
| Schedule            | always          |     |
| Service             | HTTP            | X + |
|                     | FTP             | X   |
|                     | SSH             | X   |
| Action              | ACCEPT          |     |

**Firewall / Network Options**

☐ NAT

☐ Web Cache

☐ WAN Optimization

**Security Profiles**

☒ Antivirus

☐ Web Filter

☐ Application Control

☒ IPS

☐ Email Filter

☐ DLP Sensor

☐ VoIP

☐ ICAP

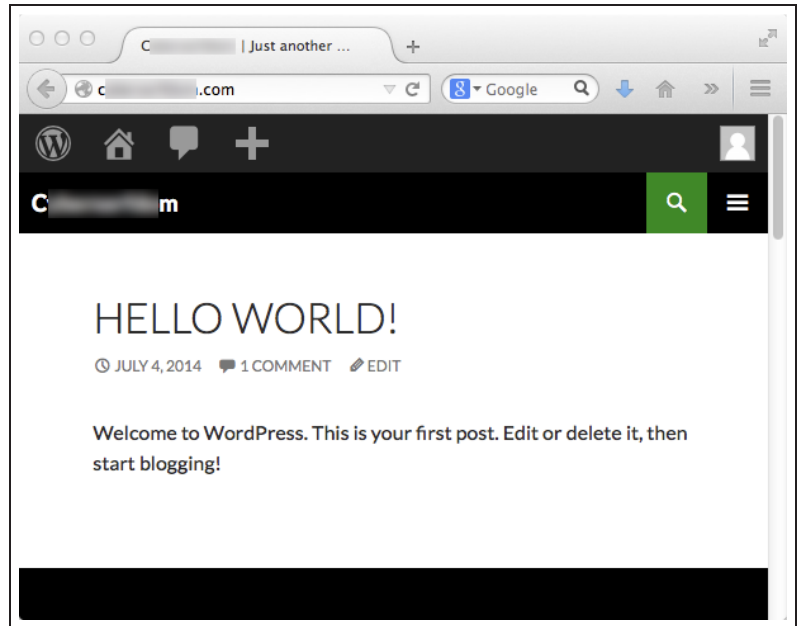
Proxy Options

☒ SSL Inspection

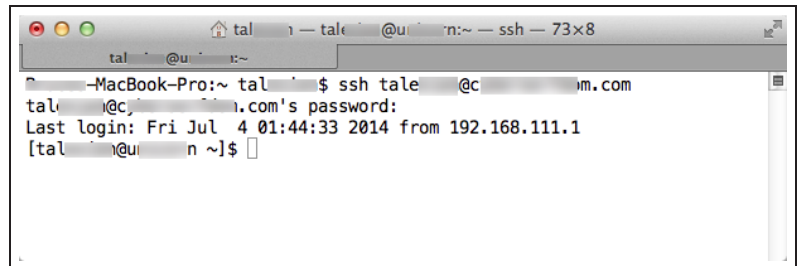
|         |  |
|---------|--|
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |
| default |  |

## 4. Results

To ensure that TCP port 80 is open, connect to the web server on the other side of the firewall.

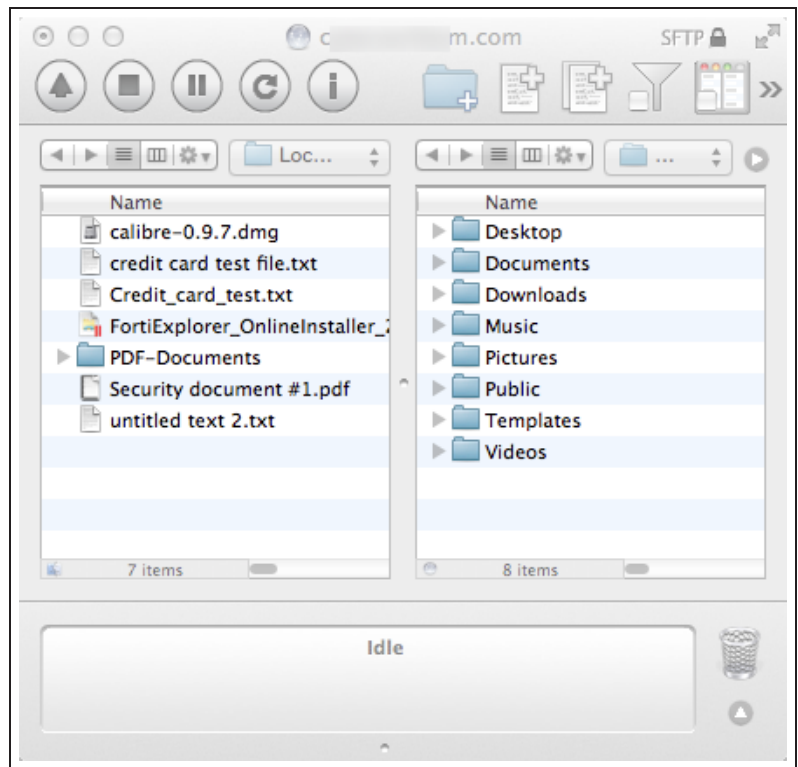


To ensure that TCP port 22 is open, connect to the SSH server on the other side of the firewall.



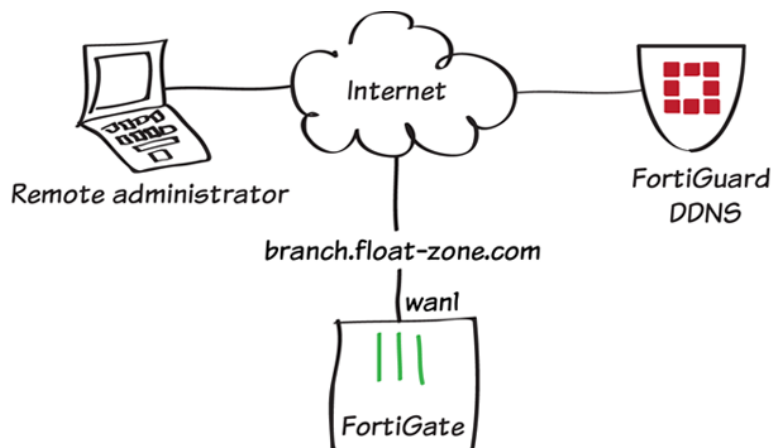


To ensure that TCP port 21 is open, use an FTP client to connect to the FTP server on the other side of the firewall.



For further reading, check out [Virtual IPs](#) in the [FortiOS 5.2 Handbook](#).

# FortiGuard DDNS



In this example, you will use FortiGuard Dynamic Domain Name Service (DDNS) to allow a remote administrator to access your FortiGate's Internet-facing interface using a domain name that remains constant, even when its IP address changes.

*An active FortiCare Support Contract is required to use FortiGuard DDNS.*

## 1. Limited administrative access to trusted hosts

Go to **System > Admin > Administrators** and edit the default *admin* account.

Enable **Restrict this Administrator Login from Trusted Hosts Only**. Add the required internal or remote devices as Trusted Hosts. You can also set an entire subnet as the trusted host, using /24 as the netmask.

| Restrict this Administrator Login from Trusted Hosts Only |                    |
|---|--------------------|
| Trusted Host #1   | 192.168.200.110/32 |
| Trusted Host #2   | 172.20.120.100/32  |
| Trusted Host #3   | 0.0.0.0/0.0.0.0    |
| IPv6 Trusted Host #1                                      | ::/0               |
| IPv6 Trusted Host #2                                      | ::/0               |
| IPv6 Trusted Host #3                                      | ::/0               |

## 2. Enabling HTTP/HTTPS access on the Internet-facing interface

Go to **System > Network > Interfaces** and edit the Internet-facing interface (typically *wan1*).

Make sure that **Administrative Access** is allowed for HTTPS.

| Administrative Access                     |  |                                     |  |                                 |
|---|--|-------------------------------------|--|---------------------------------|
| <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> PING | <input type="checkbox"/> HTTP       | <input checked="" type="checkbox"/> FMG-Access | <input type="checkbox"/> CAPWAP |
| <input type="checkbox"/> SSH              | <input type="checkbox"/> SNMP            | <input type="checkbox"/> FCT-Access |  |                                 |

## 2. Setting up FortiGuard DDNS

Go to **System > Network > DNS** and enable FortiGuard DDNS.

Set **Interface** to your Internet-facing interface, select a **Server**, and select a **Unique Location** that will be used in the domain name.

The FortiGuard DDNS service will verify that the resulting domain name is unique and valid. If it is valid, select **Apply**. The domain name is now displayed, with the current IP address of the interface.

You can click the domain name to browse to the address with a web server.

| Enable FortiGuard DDNS |  |
|------------------------|--|
| Interface              | wan1                                   |
| Server                 | float-zone.com                         |
| Unique Location        | branch                                 |
| Domain                 | branch.float-zone.com (172.20.120.236) |

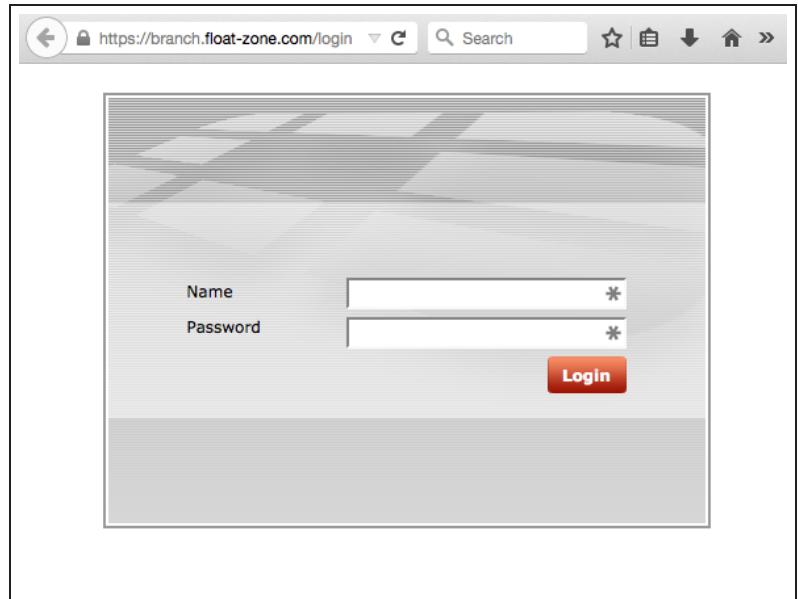
You can also configure FortiGuard DDNS by using the following CLI commands:

```
config system ddns
edit 0
set ddns-server FortiGuardDDNS
set ddns-domain "branch.float-zone.com"
set monitor-interface wan1
end
end
```

### 3. Results

Browse to the domain name assigned to the interface, using HTTPS (in the example, <https://branch.float-zone.com>).

The FortiGate login screen will appear.



Go to **System > Network > Interfaces** and edit the Internet-facing interface.

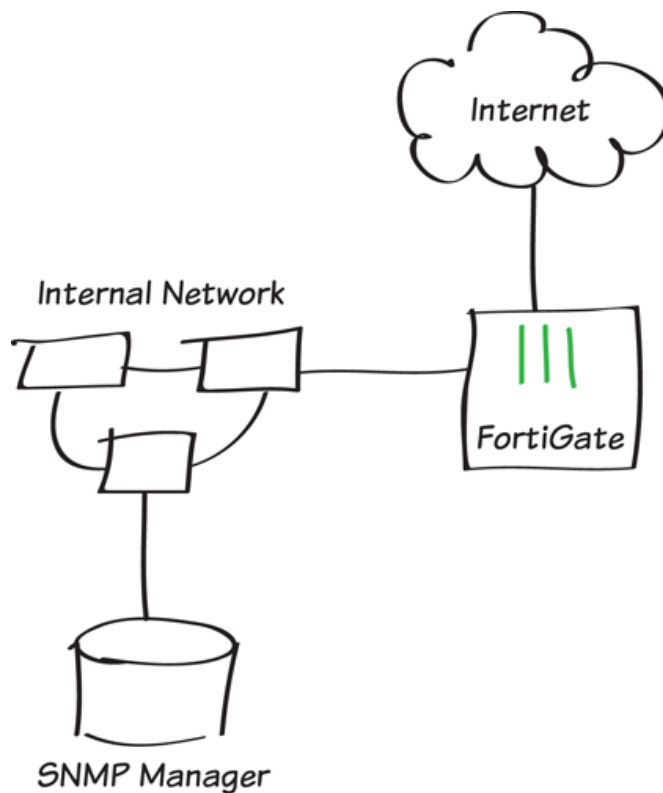
Change the interface's **IP Address/Netmask**.

|                 |  |
|-----------------|--|
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device |
| IP/Network Mask | <input type="text" value="172.20.120.237/255.255.255.0"/>  |

You will still be able to access the interface using the domain name.

For further reading, check out [Dynamic DNS configuration](#) in the [FortiOS 5.2 Handbook](#).

# SNMP monitoring



In this example, you configure the FortiGate SNMP agent and an example SNMP manager so that the SNMP manager can get status information from the FortiGate unit and so that the FortiGate unit can send traps to the SNMP manager.

The Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers.

# 1. Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**. Enable the **SNMP Agent** and add any necessary information.

SNMP Agent

☒ Enable

Description

Company FortiGate unit

Location

Head Office, server room

Contact

admin@company.com

Apply

SNMP v1/v2c

Create New

Edit

Delete

|                          | Community Name | Queries                             | Traps                               | Enable                              |
|--------------------------|----------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | FortiGates     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

SNMP v3

Create New

Edit

Delete

|  | User Name | Security Level | Notification Host | Queries |
|--|-----------|----------------|-------------------|---------|
|--|-----------|----------------|-------------------|---------|

FortiGate SNMP MIB

Download FortiGate MIB File

Download Fortinet Core MIB File

Under SNMP v1/v2c, create a new community.

Add the IP address of SNMP manager (in the example, 192.168.1.114/32). If required, change the query and trap ports to match the SNMP manager.

You can add multiple SNMP managers, or set the **IP address/Netmask** to 0.0.0.0/0.0.0.0 and the **Interface** to **ANY**, so that any SNMP manager on any network connected to the FortiGate unit can use this SNMP community and receive traps from the FortiGate unit.

Enable the **SNMP Events** (traps) that you need. In most cases, leave them all enabled.

Edit SNMP Community

Community NameFortiGates

Hosts:

| IP Address/Netmask            | Interface | Delete |
|-------------------------------|-----------|--------|
| 192.168.1.114/255.255.255.255 | ANY       |        |

Add

Queries:

| Protocol | Port | Enable                              |
|----------|------|-------------------------------------|
| v1       | 161  | <input checked="" type="checkbox"/> |
| v2c      | 161  | <input checked="" type="checkbox"/> |

Traps:

| Protocol | Local | Remote | Enable                              |
|----------|-------|--------|-------------------------------------|
| v1       | 162   | 162    | <input checked="" type="checkbox"/> |
| v2c      | 162   | 162    | <input checked="" type="checkbox"/> |

SNMP Events

☒ CPU usage is high

☒ Memory is low

☒ Log disk space is low

☒ Interface IP is changed

☒ VPN tunnel up

☒ VPN tunnel down

☒ WiFi Controller AP up

☒ WiFi Controller AP down

☒ HA cluster status is changed

☒ HA heartbeat failure

☒ HA member up

☒ HA member down

☒ Virus detected

☒ Matched file pattern detected

☒ Fragmented email detected

☒ Oversized file/email detected

☒ Oversized file/email blocked

☒ Oversized file/email passed

☒ AV bypass happens</div>

98

Getting Started

## 2. Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces** and edit the interface connected to the same network as the SNMP manager.

Enable **SNMP** for **Administrative Access**.

**Edit Interface**

Interface Name: internal(00:09:0F:DF:43:48)  
Alias:   
Link Status: Up   
Type: Physical Interface

Addressing mode: ☒ Manual ☐ DHCP ☐ PPPoE ☐ Dedicate to Extension Device  
IP/Network Mask:

Administrative Access: ☒ HTTPS ☒ PING ☒ HTTP ☒ FMG-Access ☒ CAPWAP  
☒ SSH ☒ SNMP ☐ FCT-Access  
☐ Auto IPsec Request

## 3. Downloading the Fortinet MIB files to and configuring an example SNMP manage

Two types of MIB files are available for FortiGate units: the Fortinet MIB and the FortiGate MIB. The Fortinet MIB contains traps, fields, and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields, and information that is specific to FortiGate units.

Go to **System > Config > SNMP** and select **Download FortiGate SNMP MIB File** and **Download Fortinet Core MIB File**. Configure the SNMP manager to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs.

SNMP Agent: ☒ Enable  
Description:   
Location:   
Contact:   
**Apply**

**SNMP v1/v2c**

|                          | Community Name | Queries | Traps | Enable                              |
|--------------------------|----------------|---------|-------|-------------------------------------|
| <input type="checkbox"/> | FortiGates     |         |       | <input checked="" type="checkbox"/> |

**SNMP v3**

|  | User Name | Security Level | Notification Host | Queries |
|--|-----------|----------------|-------------------|---------|
|--|-----------|----------------|-------------------|---------|

**FortiGate SNMP MIB**

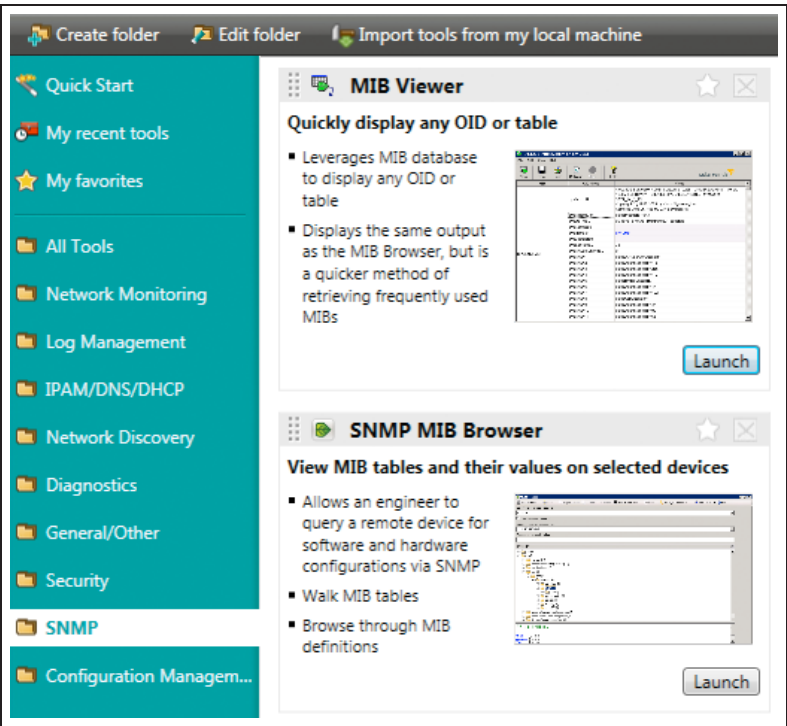
[Download FortiGate MIB File](#)  
[Download Fortinet Core MIB File](#)



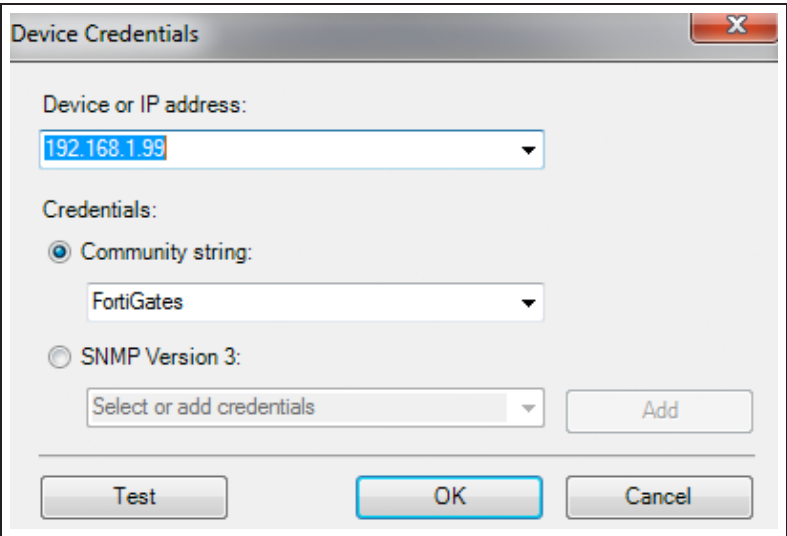
## 4. Results

This example uses the SolarWinds SNMP trap viewer.

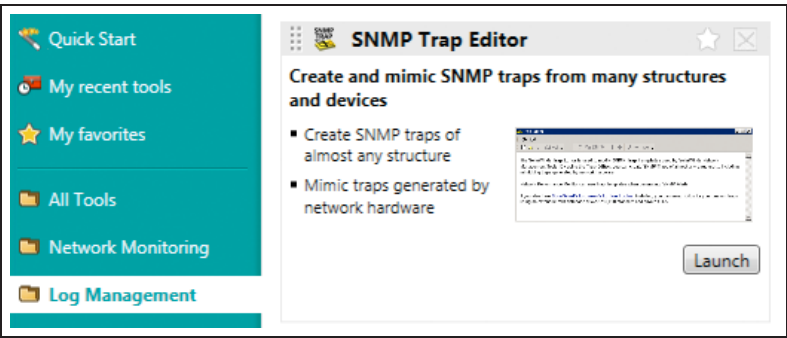
In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.



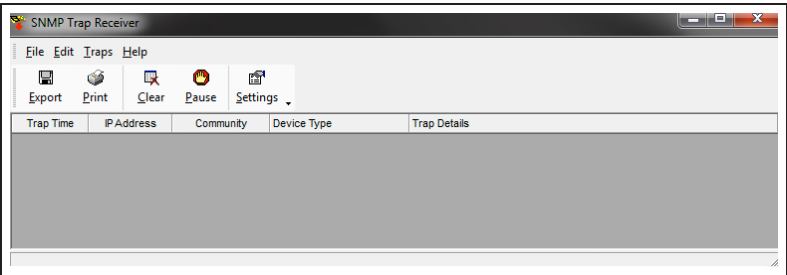
Choose **Select Device**, enter the IP address of the FortiGate unit, and choose the appropriate community string credentials.



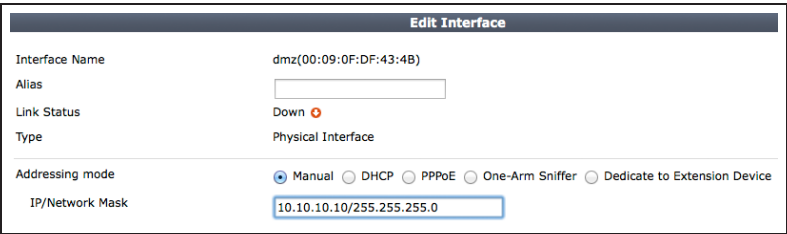
Open the **SNMP Trap Receiver** and select **Launch**.



The SNMP Trap Receiver will appear.



On the FortiGate unit, perform an action to trigger a trap (for example, change the IP address of the DMZ interface).

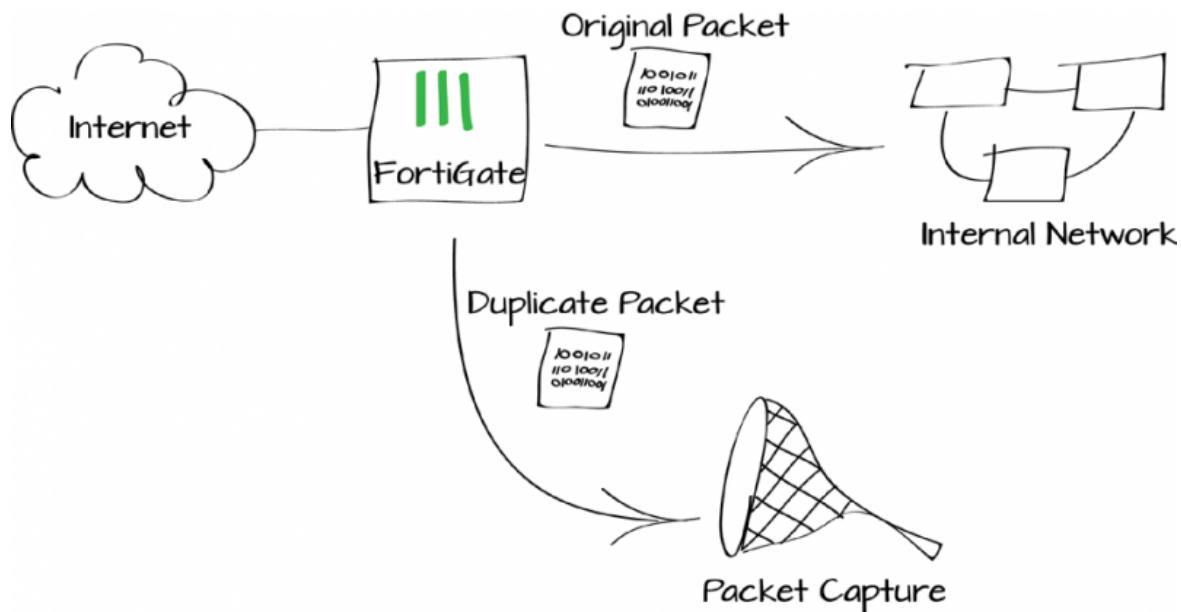


Verify that the SNMP manager receives the trap.

| Trap Time             | IP Address   | Community  | Device Type         | Trap Details  |
|-----------------------|--------------|------------|---------------------|---|
| 08-Mar-13<br>10:49 AM | 192.168.1.99 | FortiGates |                     | sysUpTime = 6976332<br>snmpTrapOID = fnTrapInfg.1.3.0.201<br>fnTrapInfg.1.1.1 = FG100D3G12801361<br>sysName = FG100D3G12801361<br>ifIndex = 2   |
| 08-Mar-13<br>10:49 AM | 192.168.1.99 | FortiGates | fnTrapSystem.1.1004 | sysUpTime = 6976332<br>snmpTrapOID = fnTrapSystem.1.1004.0.201<br>fnTrapInfg.1.1.1 = FG100D3G12801361<br>sysName = FG100D3G12801361<br>ifIndex = 2<br>experimental.1057.1 = 192.168.1.99  |
| 08-Mar-13<br>10:49 AM | 192.168.1.99 | FortiGates |                     | sysUpTime = 6976332<br>snmpTrapOID = fnTrapSystem.6.0.1004<br>fnTrapInfg.1.1.1 = FG100D3G12801361<br>ifName.2 = dmz<br>fnTrapSystem.6.2.1 = 10.10.10.1<br>fnTrapSystem.6.2.2 = 255.255.255.0  |
| 08-Mar-13<br>10:49 AM | 192.168.1.99 | FortiGates | fnTrapSystem.1.1004 | sysUpTime = 6976332<br>snmpTrapOID = fnTrapSystem.1.1004.0.1004<br>fnTrapInfg.1.1.1 = FG100D3G12801361<br>ifName.2 = dmz<br>fnTrapSystem.6.2.1 = 10.10.10.1<br>fnTrapSystem.6.2.2 = 255.255.255.0<br>experimental.1057.1 = 192.168.1.99 |

For further reading, check out **SNMP** in the **FortiOS 5.2 Handbook**.

# Packet capture



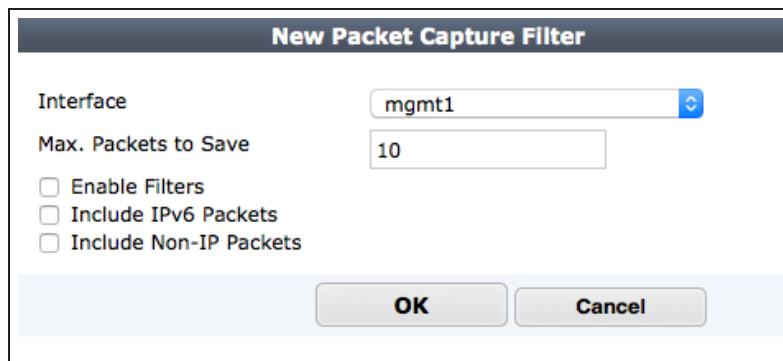
In this example, you will set up and run some basic packet capture filters on your FortiGate and download and view the resulting .pcap file.

You can use packet capturing to learn about network activity seen by your FortiGate by creating and saving packet capture filters that define the packets to capture. You can then run these filters at any time, download the resulting .pcap (packet capture) file, and use a tool like Wireshark to analyze the results.

## 1. Creating packet capture filters

Go to **System > Network > Packet Capture** and create a new filter. Below are a few examples of different filters you can use.

The simplest filter just captures all of the packets received by an interface. This example captures 10 packets received by the mgmt1 interface.

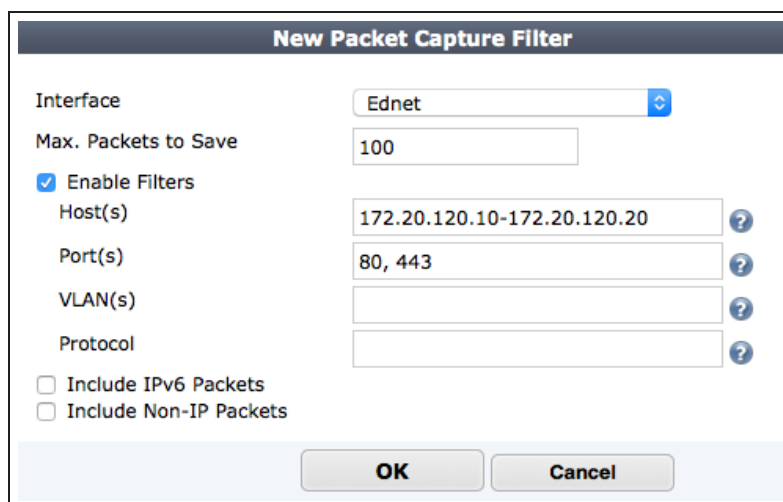


The dialog box titled "New Packet Capture Filter" has a dark header. It contains the following fields and options:

- Interface:** A dropdown menu with "mgmt1" selected.
- Max. Packets to Save:** A text input field containing "10".
- Options:** Three checkboxes, all of which are unchecked:
  - ☐ Enable Filters
  - ☐ Include IPv6 Packets
  - ☐ Include Non-IP Packets
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

You can select **Enable Filters** to restrict the packets to capture.

This filter captures 100 HTTP and HTTPS packets (port 80 and 443) received by the Ednet wireless interface that have a source or destination address in the range 172.20.120.10 to 172.20.120.20.

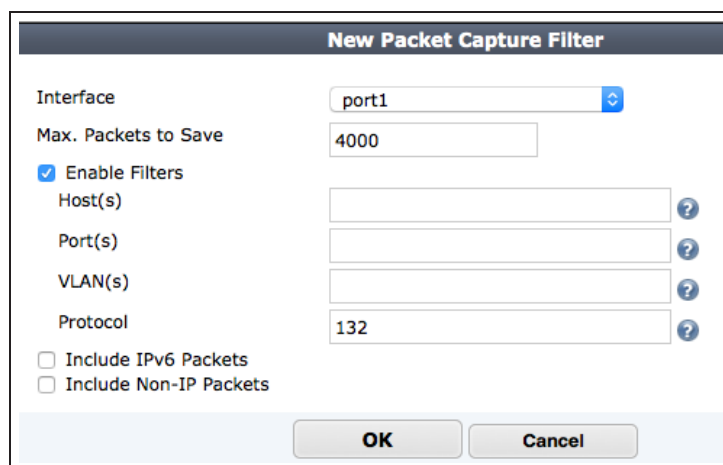


The dialog box titled "New Packet Capture Filter" has a dark header. It contains the following fields and options:

- Interface:** A dropdown menu with "Ednet" selected.
- Max. Packets to Save:** A text input field containing "100".
- Options:** Three checkboxes:
  - ☒ Enable Filters
  - ☐ Include IPv6 Packets
  - ☐ Include Non-IP Packets
- Filter Fields:** When "Enable Filters" is checked, several fields appear with question mark icons to their right:
  - Host(s):** A text input field containing "172.20.120.10-172.20.120.20".
  - Port(s):** A text input field containing "80, 443".
  - VLAN(s):** An empty text input field.
  - Protocol:** An empty text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

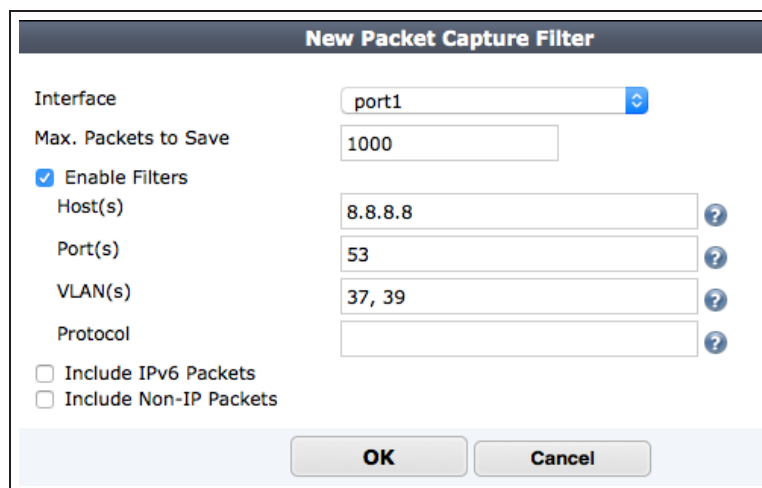
This filter captures the first 4000 Stream Control Transmission Protocol (SCTP) packets received by the port1 interface.

*Protocols are identified using IP protocol numbers; for example, SCTP is protocol 132.*



The 'New Packet Capture Filter' dialog box is shown. It has a title bar 'New Packet Capture Filter'. The 'Interface' dropdown is set to 'port1'. 'Max. Packets to Save' is set to '4000'. The 'Enable Filters' checkbox is checked. Below it, 'Host(s)', 'Port(s)', and 'VLAN(s)' are empty text boxes, each with a help icon. The 'Protocol' dropdown is set to '132' with a help icon. At the bottom, there are two unchecked checkboxes: 'Include IPv6 Packets' and 'Include Non-IP Packets'. At the very bottom are 'OK' and 'Cancel' buttons.

This filter captures the first 1000 DNS packets querying the Google DNS server (IP address 8.8.8.8) with VLAN IDs 37 or 39.



The 'New Packet Capture Filter' dialog box is shown. It has a title bar 'New Packet Capture Filter'. The 'Interface' dropdown is set to 'port1'. 'Max. Packets to Save' is set to '1000'. The 'Enable Filters' checkbox is checked. Below it, 'Host(s)' is set to '8.8.8.8', 'Port(s)' is set to '53', and 'VLAN(s)' is set to '37, 39'. Each of these three fields has a help icon. The 'Protocol' dropdown is empty with a help icon. At the bottom, there are two unchecked checkboxes: 'Include IPv6 Packets' and 'Include Non-IP Packets'. At the very bottom are 'OK' and 'Cancel' buttons.

## 2. Results

Running packet capture filters may affect FortiGate performance.

Go to **System > Network > Packet Capture**, choose a filter, and select the **Play** icon. You can watch the filter capture packets. When the number of packets specified in the filter are captured the filter stops.

You can stop and restart multiple filters at any time.

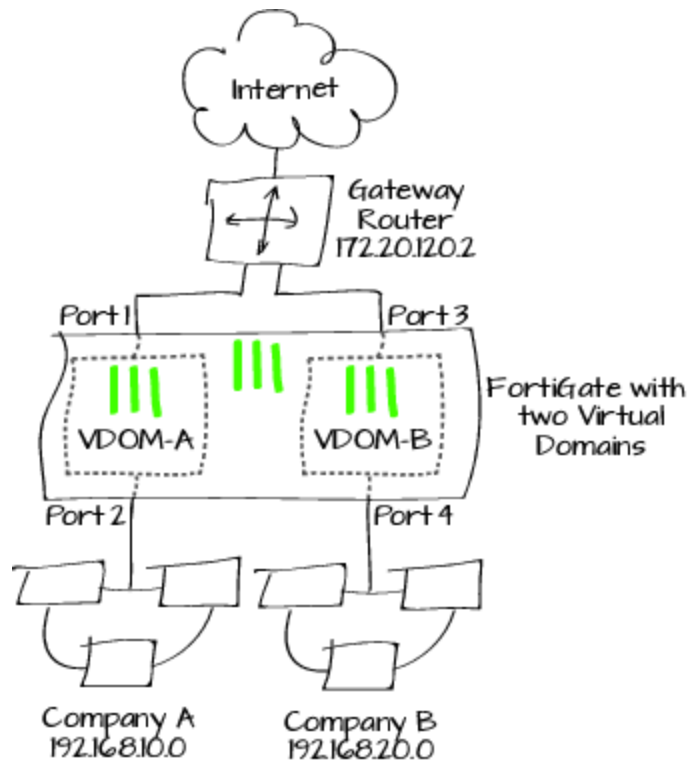
Download any saved .pcap file to your computer. You can open the file with a .pcap file viewer like Wireshark.

| Create New Edit Delete |                 |           |                  |                        |
|------------------------|-----------------|-----------|------------------|------------------------|
| Interface              | Filter Criteria | # Packets | Max Packet Count | Progress               |
| mgmt1                  |                 | 10        | 10               | <div><div></div></div> |
| Ednet                  | host=10.10.10.2 | 100       | 100              | <div><div></div></div> |
| port1                  | proto=132       | 0         | 4000             | <div><div></div></div> |
| Ednet                  | proto=17        | 1310      | 200              | <div><div></div></div> |

| No. | Time      | Source         | Destination    | Protocol  | Length | Info  |
|-----|-----------|----------------|----------------|-----------|--------|---|
| 1   | 0.000000  | 10.10.80.3     | 209.148.192.25 | TCP       | 55     | 53343->80 [ACK] Seq=1 Ack=1 win=63744 Len=1               |
| 2   | 0.014731  | 209.148.192.25 | 10.10.80.3     | TCP       | 66     | 80->53343 [ACK] Seq=1 Ack=2 win=16872 Len=0 SLE=1 SRE=2   |
| 3   | 45.050679 | 74.125.226.121 | 10.10.80.3     | TCP       | 54     | 80->53224 [FIN, ACK] Seq=1 Ack=1 win=43952 Len=0          |
| 4   | 45.051602 | 10.10.80.3     | 74.125.226.121 | TCP       | 54     | 53224->80 [ACK] Seq=1 Ack=2 win=64153 Len=0               |
| 5   | 45.051817 | 10.10.80.3     | 74.125.226.121 | TCP       | 54     | 53224->80 [FIN, ACK] Seq=1 Ack=2 win=64153 Len=0          |
| 6   | 45.070072 | 74.125.226.121 | 10.10.80.3     | TCP       | 54     | 80->53224 [ACK] Seq=2 Ack=2 win=43952 Len=0               |
| 7   | 46.696955 | 10.10.80.3     | 173.192.82.195 | TCP       | 62     | 53446->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 8   | 46.748411 | 173.192.82.195 | 10.10.80.3     | TCP       | 62     | 80->53446 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 |
| 9   | 46.749380 | 10.10.80.3     | 173.192.82.195 | TCP       | 54     | 53446->80 [ACK] Seq=1 Ack=1 win=64240 Len=0               |
| 10  | 46.753544 | 10.10.80.3     | 173.192.82.195 | HTTP      | 1511   | GET /ws/2/thread/3293935889? HTTP/1.1                     |
| 11  | 46.802775 | 173.192.82.195 | 10.10.80.3     | TCP       | 54     | 80->53446 [ACK] Seq=1 Ack=1458 win=17484 Len=0            |
| 12  | 46.803950 | 173.192.82.195 | 10.10.80.3     | HTTP      | 275    | HTTP/1.1 101 Switching Protocols                          |
| 13  | 47.013156 | 10.10.80.3     | 173.192.82.195 | TCP       | 54     | 53446->80 [ACK] Seq=1458 Ack=222 win=64019 Len=0          |
| 14  | 47.047410 | 173.192.82.195 | 10.10.80.3     | Websocket | 275    | (TCP: Acknowledgment) Websocket (unknown) opcode          |

For further reading, check out [Monitoring](#) in the [FortiOS 5.2 Handbook](#).

# VDOM configuration



This example illustrates how to use VDOMs to host two FortiOS instances on a single FortiGate unit.

Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct Internet services. Each company has its own VDOM, IP address, and internal network.

A video of this recipe is available [here](#).



## 1. Switching to VDOM mode and creating two VDOMS

Go to **System > Dashboard > Status**.


In the **System Information** widget, find **Virtual Domain** and select **Enable**.


You will be required to re-login after enabling **Virtual Domain** due to the GUI menu options changing.

| ▼ System Information  |  |
|-----------------------|--|
| HA Status             | Standalone [Configure]                         |
| Host Name             | FGT60C3G10016011 [Change]                      |
| Serial Number         | FGT60C3G10016011                               |
| System Time           | Wed Dec 10 11:39:34 2014 (FortiGuard) [Change] |
| Firmware Version      | v5.2.2,build642 (GA) [Update]                  |
| System Configuration  | [Backup] [Restore] [Revisions]                 |
| Current Administrator | admin [Change Password] /1 in Total [Details]  |
| Uptime                | 20 day(s) 1 hour(s) 58 min(s)                  |
| Virtual Domain        | Enabled [Disable]                              |

Go to **Global > VDOM > VDOM**.

Create two VDOMS: *VDOM-A* and *VDOM-B*. Leave both VDOMs as **Enabled**, with **Operation Mode** set to **NAT**.

|                |   |
|----------------|---|
| Name           | <input type="text" value="VDOM-A"/>   |
| Enable         | <input checked="" type="checkbox"/>   |
| Operation Mode |  NAT ▼ |
| Comments       | <input type="text" value="Write a comment..."/> 0/255                                   |

|                |   |
|----------------|---|
| Name           | <input type="text" value="VDOM-B"/>   |
| Enable         | <input checked="" type="checkbox"/>   |
| Operation Mode |  NAT ▼ |
| Comments       | <input type="text" value="Write a comment..."/> 0/255                                     |

## 2. Assigning interfaces to each VDOM

Go to **Global > Network > Interfaces**.

Edit **port1** and add it to VDOM-A. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, *172.20.120.10/255.255.255.0*).

|                 |  |
|-----------------|--|
| Name            | port1(00:09:0F:B0:EB:F0)   |
| Alias           |  |
| Link Status     | Down   |
| Type            | Physical Interface   |
| Virtual Domain  | VDOM-A   |
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicate to FortiAP/FortiSwitch |
| IP/Network Mask | 172.20.120.10/255.255.255.0  |
| IPv6 Address    | ::/0   |

Edit **port2** and add it to VDOM-A. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.10.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.

| Name                       | port2(00:09:0F:B0:EB:F1)   |             |        |              |                |
|----------------------------|--|-------------|--------|--------------|----------------|
| Alias                      |  |             |        |              |                |
| Link Status                | Down   |             |        |              |                |
| Type                       | Physical Interface   |             |        |              |                |
| Virtual Domain             | VDOM-A   |             |        |              |                |
| Addressing mode            | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP/FortiSwitch                                 |             |        |              |                |
| IP/Network Mask            | 192.168.10.1/255.255.255.0   |             |        |              |                |
| IPv6 Address               | ::/0   |             |        |              |                |
| Administrative Access      | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP |             |        |              |                |
|                            | <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access  |             |        |              |                |
| IPv6 Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP                       |             |        |              |                |
|                            | <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET   |             |        |              |                |
| DHCP Server                | <input checked="" type="checkbox"/> Enable   |             |        |              |                |
| Address Range              | <div>Create New Edit Delete</div> <table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>192.168.10.2</td><td>192.168.10.254</td></tr></tbody></table>     | Starting IP | End IP | 192.168.10.2 | 192.168.10.254 |
| Starting IP                | End IP   |             |        |              |                |
| 192.168.10.2               | 192.168.10.254   |             |        |              |                |
| Netmask                    | 255.255.255.0  |             |        |              |                |

Edit **port3** and add it to VDOM-B. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, *172.20.120.20/255.255.255.0*).

|                 |  |
|-----------------|--|
| Name            | port3(00:09:0F:B0:EB:F2)   |
| Alias           |  |
| Link Status     | Down   |
| Type            | Physical Interface   |
| Virtual Domain  | VDOM-B   |
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicate to FortiAP/FortiSwitch |
| IP/Network Mask | 172.20.120.20/255.255.255.0  |
| IPv6 Address    | ::/0   |

Edit **port4** and add it to VDOM-B. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.20.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable *DHCP Server*.

| Interface Name        | internal4(00:09:0F:DF:43:4D)   |             |        |              |                |
|-----------------------|--|-------------|--------|--------------|----------------|
| Alias                 |  |             |        |              |                |
| Link Status           | Down   |             |        |              |                |
| Type                  | Physical Interface   |             |        |              |                |
| Virtual Domain        | VDOM-B   |             |        |              |                |
| Addressing mode       | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device   |             |        |              |                |
| IP/Network Mask       | 192.168.20.1/255.255.255.0   |             |        |              |                |
| Administrative Access | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access<br><input type="checkbox"/> Auto IPsec Request |             |        |              |                |
| DHCP Server           | <input checked="" type="checkbox"/> Enable   |             |        |              |                |
| Address Range         | <div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>192.168.20.2</td><td>192.168.20.254</td></tr></tbody></table></div>   | Starting IP | End IP | 192.168.20.2 | 192.168.20.254 |
| Starting IP           | End IP   |             |        |              |                |
| 192.168.20.2          | 192.168.20.254   |             |        |              |                |
| Netmask               | 255.255.255.0  |             |        |              |                |

### 3. Creating administrators for each VDOM

Go to **Global > Admin > Administrators**.

Create an administrators for VDOM-A, called *a-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof\_admin**.

|                  |   |
|------------------|---|
| Administrator    | a-admin   |
| Type             | <input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI |
| Password         | .....   |
| Confirm Password | .....   |
| Comments         | <div>Write a comment... 0/255</div>   |
| Admin Profile    | prof_admin  |
| Virtual Domain   | VDOM-A  |

Create an administrators for VDOM-B, called *b-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof\_admin**.

Make sure to remove the **root** VDOM from both administrator accounts.

|                  |   |
|------------------|---|
| Administrator    | b-admin   |
| Type             | <input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI |
| Password         | .....   |
| Confirm Password | .....   |
| Comments         | <div>Write a comment... 0/255</div>   |
| Admin Profile    | prof_admin  |
| Virtual Domain   | VDOM-B  |

## 4. Creating a basic configuration for VDOM-A

Go to **Virtual Domains** and select **VDOM-A**.

Go to **System > Network > Routing**.

Create a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port1**, and set **Gateway** to the IP of the gateway router (in the example, *172.20.120.2*).

Connect a PC to port2. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-A using the a-admin account (in the example, *192.168.10.1*).

Go to **Policy & Objects > Policy > IPv4**

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Ensure **NAT** is turned **On**.

|                     |  |
|---------------------|--|
| Destination IP/Mask | <input type="text" value="0.0.0.0/0.0.0.0"/>   |
| Device              | <input type="text" value="internal1 (port1)"/> |
| Gateway             | <input type="text" value="172.20.120.2"/>      |

|                     |  |
|---------------------|--|
| Incoming Interface  | <input type="text" value="internal2 (port2)"/> |
| Source Address      | <input type="text" value="all"/>               |
| Source User(s)      | <input type="text" value="Click to add..."/>   |
| Source Device Type  | <input type="text" value="Click to add..."/>   |
| Outgoing Interface  | <input type="text" value="internal1 (port1)"/> |
| Destination Address | <input type="text" value="all"/>               |
| Schedule            | <input type="text" value="always"/>            |
| Service             | <input type="text" value="ALL"/>               |
| Action              | <input type="text" value="ACCEPT"/>            |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 5. Creating a basic configuration for VDOM-B

If you have logged out of the FortiGate unit, log back in.

Go to **Virtual Domains** and select **VDOM-B**.

Go to **System > Network > Routing**

Create a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port3**, and set **Gateway** to the IP of the gateway router (in the example, *172.20.120.2*).

Connect a PC to port4. Using HTTPS protocol, browse to the IP set for port4 and log into VDOM-B using the a-admin account (in the example, *https://192.168.10.1*).

Go to **Policy & Objects > Policy > IPv4**

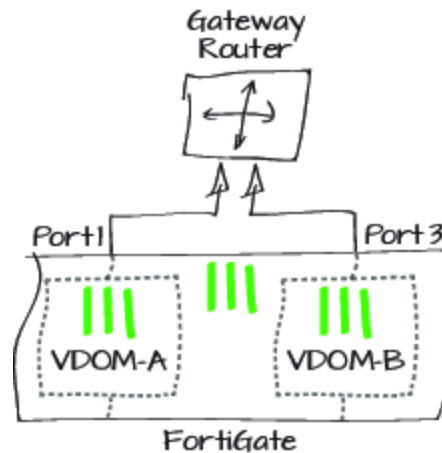
Create a policy to allow Internet access. Set **Incoming Interface** to **port4** and **Outgoing Interface** to **port3**. Ensure **NAT** is turned **On**.

|                     |  |
|---------------------|--|
| Destination IP/Mask | <input type="text" value="0.0.0.0/0.0.0.0"/>   |
| Device              | <input type="text" value="internal3 (port3)"/> |
| Gateway             | <input type="text" value="172.20.120.2"/>      |

|   |  |
|---|--|
| Incoming Interface  | <input type="text" value="internal4 (port4)"/> |
| Source Address  | <input type="text" value="all"/>               |
| Source User(s)  | <input type="text" value="Click to add..."/>   |
| Source Device Type  | <input type="text" value="Click to add..."/>   |
| Outgoing Interface  | <input type="text" value="internal3 (port3)"/> |
| Destination Address   | <input type="text" value="all"/>               |
| Schedule  | <input type="text" value="always"/>            |
| Service   | <input type="text" value="ALL"/>               |
| Action  | <input type="text" value="ACCEPT"/>            |
| <b>Firewall / Network Options</b>                               |  |
| <input checked="" type="checkbox"/> ON NAT                      |  |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port            |
| <input type="radio"/> Use Dynamic IP Pool                       | <input type="text" value="Click to add..."/>   |

## 6. Connecting the gateway router

Connect port 1 and port3 of the FortiGate unit to the gateway router to allow Internet traffic to flow.

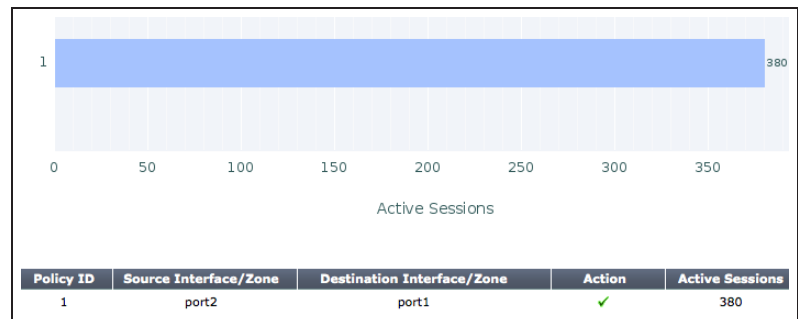


## 7. Results

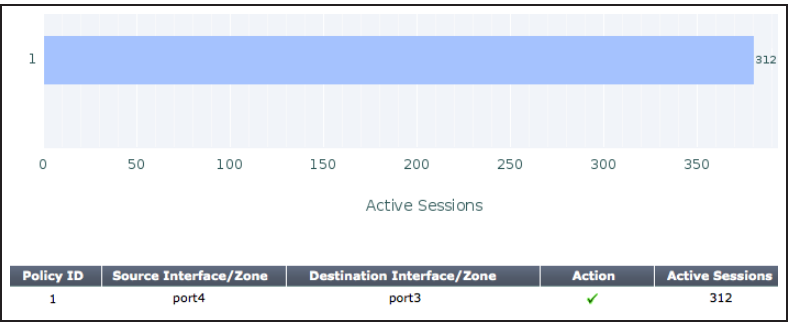
Connect to the Internet from the company A and company B networks and then log into the FortiGate unit

Go to **Virtual Domains** and select **VDOM-A**.

Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-A.

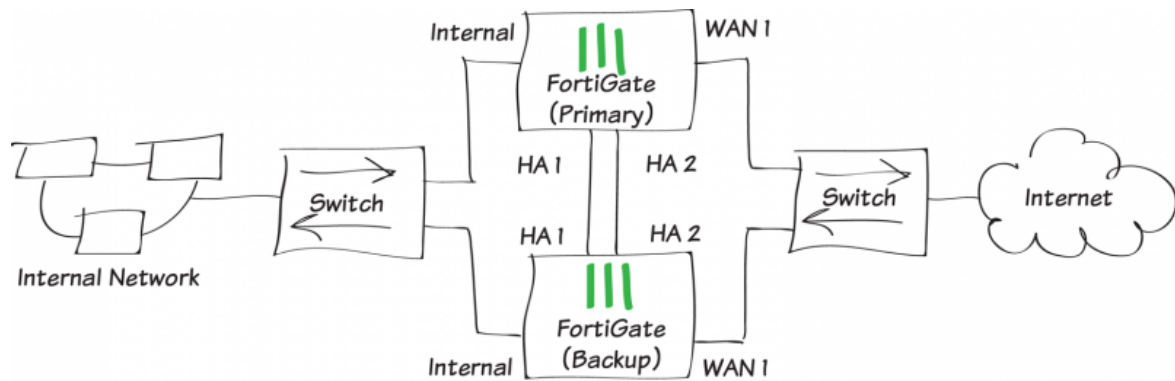


Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-B.



For further reading, check out [Virtual Domains](#) in the [FortiOS 5.2 Handbook](#).

# High Availability with two FortiGates



In this recipe, a backup FortiGate unit will be installed and connected to a FortiGate unit that has previously been installed to provide redundancy if the primary FortiGate unit fails. This set up, called High Availability (HA), improves network reliability.

If you have not already installed a FortiGate, see [Installing a FortiGate in NAT/Route mode](#).

A video of this recipe is available [here](#).



## 1. Adding the backup FortiGate unit and configuring HA

If the FortiGates in the cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to the new FortiGate unit before adding it to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.

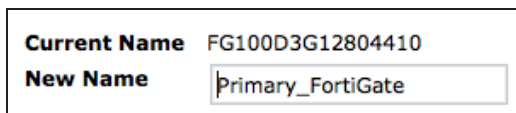
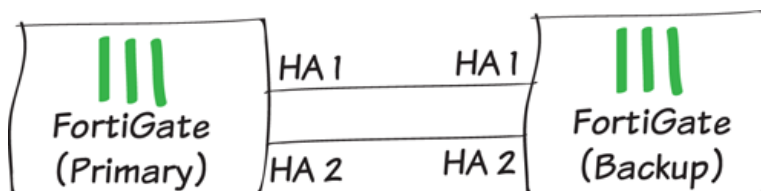
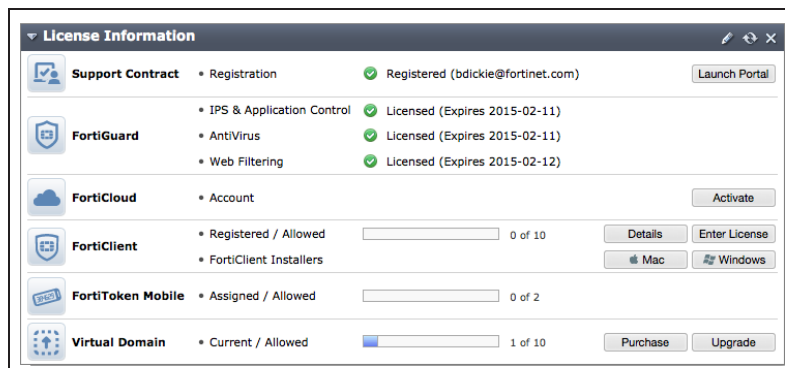
You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.

Connect your network as shown in the initial diagram, with Ethernet cables connecting the HA heartbeat interfaces of the two FortiGate units. If your FortiGate unit does not have dedicated HA heartbeat interfaces, you can use different interfaces, provided they are not used for any other function.

A switch must be used between the FortiGates and Internet, and another is required between the FortiGates and the internal network, as shown in the network diagram for this recipe.

Connect to the primary FortiGate and go to **System > Dashboard > Status** and locate the **System Information** widget.

Change the unit's **Host Name** to identify it as the primary FortiGate.



In the **System Information** widget, configure **HA Status**. Set the **Mode** to **Active-Passive** and set a **Group Name** and **Password**.

Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.

Mode

Active-Passive

Device Priority

128

☐ Reserve Management Port for Cluster Member

Internal

Cluster Settings

Group Name

HA-cluster

Password

.....

☐ Enable Session Pick-up

|        | Port Monitor             | Heartbeat Interface                 |                 |
|--------|--------------------------|-------------------------------------|-----------------|
|        |                          | Enable                              | Priority(0-512) |
| dmz    | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| ha1    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <div>50</div>   |
| ha2    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <div>50</div>   |
| mgmt   | <input type="checkbox"/> |                                     |                 |
| port9  | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port10 | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port11 | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port14 | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port15 | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port16 | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| wan1   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| wan2   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |

Connect to the backup FortiGate and go to **System > Dashboard > Status**.

Change the unit's **Host Name** to identify it as the backup FortiGate.

Current Name

FG100D3G12801361

New Name

Backup\_FortiGate

Configure **HA Status** and set the **Mode** to **Active-Passive**.

Set the **Device Priority** to be lower than the primary FortiGate. Ensure that the **Group Name** and **Password** match those on the primary FortiGate.

Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.

Mode

Active-Passive

Device Priority

50

☐ Reserve Management Port for Cluster Member

dmz

Cluster Settings

Group Name

HA-cluster





Password

.....

☐ Enable Session Pick-up

|       | Port Monitor             | Heartbeat Interface                 |                 |
|-------|--------------------------|-------------------------------------|-----------------|
|       |                          | Enable                              | Priority(0-512) |
| dmz   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| ha1   | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 50              |
| ha2   | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 50              |
| mgmt  | <input type="checkbox"/> |                                     |                 |
| port1 | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| wan1  | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| wan2  | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |

Connect to the primary FortiGate and go to **System > Config > HA** to view the cluster information.

|   | Cluster Member   | Hostname          | Serial No.       | Role   | Priority |
|---|--|-------------------|------------------|--------|----------|
|   |   | Primary_FortiGate | FG100D3G12804410 | MASTER | 128      |
|  |  | Backup_FortiGate  | FG100D3G12801361 | SLAVE  | 50       |

Select **View HA Statistics** for more information on how the cluster is operating and processing traffic.

| Unit                                  | Status | Up Time    | Monitor      |                     |               |                    |
|---------------------------------------|--------|------------|--------------|---------------------|---------------|--------------------|
| Primary_FortiGate<br>FG100D3G12804410 | ✔      | 0 days     | CPU Usage    | Active Sessions     | Total Packets | Virus Detected     |
|                                       |        | 1 hours    | 1%           | 26                  | 81857         | 0                  |
|                                       |        | 44 minutes | Memory Usage | Network Utilization | Total Bytes   | Intrusion Detected |
|                                       |        | 2 seconds  | 34%          | 78 Kbps             | 27300058      | 0                  |
| Backup_FortiGate<br>FG100D3G12801361  | ✔      | 2 days     | CPU Usage    | Active Sessions     | Total Packets | Virus Detected     |
|                                       |        | 0 hours    | 0%           | 6                   | 8718576       | 0                  |
|                                       |        | 15 minutes | Memory Usage | Network Utilization | Total Bytes   | Intrusion Detected |
|                                       |        | 15 seconds | 19%          | 13 Kbps             | 2778691497    | 0                  |

## 2. Results

Normally, traffic should now be flowing through the primary FortiGate. However, if the primary FortiGate is unavailable, traffic should failover and the backup FortiGate will be used. Failover will also cause the primary and backup FortiGates to reverse roles, even when both FortiGates are available again.

To test this, ping the IP address 8.8.8.8 using a PC on the internal network. After a moment, power off the primary FortiGate

*If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.*

You will see a momentary pause in the Ping results, until traffic diverts to the backup FortiGate, allowing the Ping traffic to continue.

```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

### 3. (Optional) Upgrading the firmware for the HA cluster

For information about accessing firmware images, see [Updating your FortiGate's firmware](#).

When a new version of the FortiOS firmware becomes available, upgrading the firmware on the primary FortiGate will automatically upgrade the backup FortiGate's firmware as well.

Always review the Release Notes and Supported Upgrade Paths documentation before installing new firmware. These documents can be found at the [Fortinet Document Library](#).

Go to **System > Dashboard > Status** and view the **System Information** widget. Now that the FortiGates are in HA mode, their configuration is synchronized and the **System Information** widget displays information for both units.

Select **Backup** beside **System Configuration**. Always remember to back up your configuration before doing any firmware upgrades.

Go to **System > Dashboard > Status** and view the **System Information** widget. Select **Upgrade** beside **Firmware Version**. Find the firmware image file that you downloaded and select **OK** to upload and install the firmware build.

The firmware will load onto both the primary FortiGate unit and the backup unit.

| System Information    |  |          |
|-----------------------|--|----------|
| HA Status             | Active-Passive [Configure]                     |          |
| Cluster Name          | HA-cluster                                     |          |
| Cluster Members       | Primary_FortiGate/FG100D3G12804410             | (Master) |
|                       | Backup_FortiGate/FG100D3G12801361              | (Slave)  |
| Serial Number         | FG100D3G12804410                               |          |
| Operation Mode        | NAT [Change]                                   |          |
| System Time           | Wed Oct 29 13:27:24 2014 (FortiGuard) [Change] |          |
| Firmware Version      | v5.2.0,build0589 (GA) [Update] [Details]       |          |
| System Configuration  | [Backup] [Restore] [Revisions]                 |          |
| Current Administrator | admin [Change Password] /1 in Total [Details]  |          |
| Uptime                | 0 day(s) 0 hour(s) 22 min(s)                   |          |
| Virtual Domain        | Disabled [Enable]                              |          |

**Backup**

Backup configuration to: ☒ Local PC ☐ USB Disk

☐ Encrypt configuration file

Upgrade From

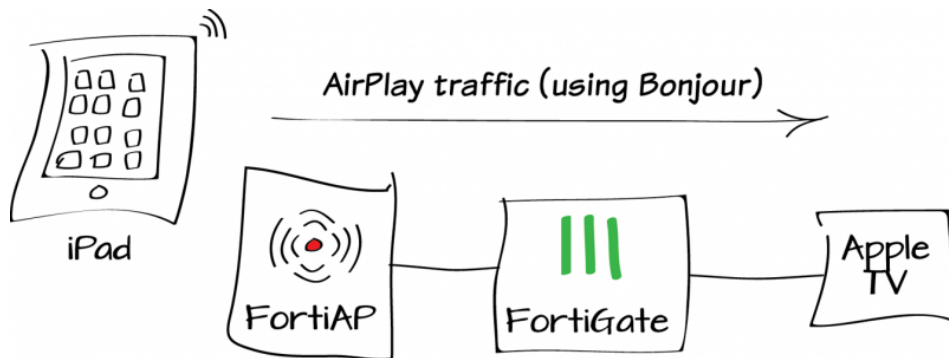
Upgrade File  FGT\_100D-v5-build0618-FORTINET.out

Go to **System > Dashboard > Status** and verify that the **System Information** widget shows the new firmware version.

| System Information    |  |          |
|-----------------------|--|----------|
| HA Status             | Active-Passive [Configure]                     |          |
| Cluster Name          | HA-cluster                                     |          |
| Cluster Members       | Primary_FortiGate/FG100D3G12804410             | (Master) |
|                       | Backup_FortiGate/FG100D3G12801361              | (Slave)  |
| Serial Number         | FG100D3G12804410                               |          |
| Operation Mode        | NAT [Change]                                   |          |
| System Time           | Wed Oct 29 13:34:57 2014 (FortiGuard) [Change] |          |
| Firmware Version      | v5.2.1,build618 (GA) [Update] [Details]        |          |
| System Configuration  | [Backup] [Restore] [Revisions]                 |          |
| Current Administrator | admin [Change Password] /1 in Total [Details]  |          |
| Uptime                | 0 day(s) 0 hour(s) 30 min(s)                   |          |
| Virtual Domain        | Disabled [Enable]                              |          |

For further reading, check out [Configuring and connecting HA clusters](#) in the [FortiOS 5.2 Handbook](#).

# AirPlay for Apple TV



In this example, you will create multicast security policies to allow AirPlay communication between an iOS device and an Apple TV through a FortiGate unit.

*Apple TV can also be connected to the Internet wirelessly. AirPlay will function from any iOS device connected to the same SSID as the Apple TV, without any configuration required on the FortiGate.*

This recipe uses a FortiAP in Tunnel mode. For more information, see [Setting up WiFi with FortiAP](#).

# 1. Enabling multicast policies

Go to **System > Config > Features**.

Select **Show More** and enable **Multicast Policy**. **Apply** the changes.



# 2. Creating AirPlay services

Go to **Policy & Objects > Objects > Services** and create a service as shown for the connection from the Apple TV to the iOS device.

|                      |  |      |      |       |
|----------------------|--|------|------|-------|
| Name                 | AirPlay - Apple TV to iOS  |      |      |       |
| Comments             |  |      |      |       |
| Service Type         | <input checked="" type="radio"/> Firewall <input type="radio"/> Explicit Proxy |      |      |       |
| Show in Service List | <input checked="" type="checkbox"/>  |      |      |       |
| Category             | Uncategorized  |      |      |       |
| Protocol Type        | TCP/UDP/SCTP   |      |      |       |
| IP/FQDN              |  |      |      |       |
| Protocol             |  | Low  | High |       |
|                      | TCP  | 5000 | -    |       |
|                      | TCP  | 7000 | -    |       |
|                      | UDP  | 1    | -    | 65535 |
| Specify Source Ports | <input type="checkbox"/>   |      |      |       |

Go to **Policy & Objects > Objects > Services** and create a service as shown for the connection from the iOS device to the Apple TV.

|                      |  |       |      |       |
|----------------------|--|-------|------|-------|
| Name                 | AirPlay - iOS to Apple TV  |       |      |       |
| Comments             |  |       |      |       |
| Service Type         | <input checked="" type="radio"/> Firewall <input type="radio"/> Explicit Proxy |       |      |       |
| Show in Service List | <input checked="" type="checkbox"/>  |       |      |       |
| Category             | Uncategorized  |       |      |       |
| Protocol Type        | TCP/UDP/SCTP   |       |      |       |
| IP/FQDN              |  |       |      |       |
| Protocol             |  | Low   | High |       |
|                      | TCP  | 5000  | -    |       |
|                      | TCP  | 7000  | -    |       |
|                      | TCP  | 7100  | -    |       |
|                      | TCP  | 49152 | -    | 50000 |
|                      | UDP  | 1     | -    | 65535 |
| Specify Source Ports | <input type="checkbox"/>   |       |      |       |



### 3. Allowing multicast between the wireless and internal networks

Go to **Policy & Objects > Policy > Multicast** and create a policy allowing local network traffic to reach the wireless network.

Set **Incoming Interface** to **lan**, **Outgoing Interface** to the wireless interface, and **Destination Address** to **Bonjour**.

*Bonjour is a default multicast address that is used by Apple devices to discover shared services on the local network. Using it in the multicast policies will allow the iOS device and Apple TV to connect to each other through the FortiGate.*

Create a second policy allowing wireless traffic to reach the internal network.

Set **Incoming Interface** to the wireless interface, **Outgoing Interface** to **lan**, and **Destination Address** to **Bonjour**.

|   |                         |
|---|-------------------------|
| Incoming Interface                                      | lan (VLAN ID: 0)        |
| Source Address  | all                     |
| Outgoing Interface                                      | wireless (SSID: myWifi) |
| Destination Address                                     | Bonjour                 |
| <input type="checkbox"/> Enable SNAT                    |                         |
| DNAT  | 0.0.0.0                 |
| Protocol  | UDP                     |
| Port Range  | 1-5353                  |
| Action  | ACCEPT                  |
| <input checked="" type="checkbox"/> Log Allowed Traffic |                         |
| <input checked="" type="checkbox"/> Enable this policy  |                         |

|   |                         |
|---|-------------------------|
| Incoming Interface                                      | wireless (SSID: myWifi) |
| Source Address  | all                     |
| Outgoing Interface                                      | lan (VLAN ID: 0)        |
| Destination Address                                     | Bonjour                 |
| <input type="checkbox"/> Enable SNAT                    |                         |
| DNAT  | 0.0.0.0                 |
| Protocol  | UDP                     |
| Port Range  | 1-5353                  |
| Action  | ACCEPT                  |
| <input checked="" type="checkbox"/> Log Allowed Traffic |                         |
| <input checked="" type="checkbox"/> Enable this policy  |                         |

## 4. Allowing airplay between the wireless and internal networks

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing traffic from the Apple TV to the iOS device.

Set **Incoming Interface** to **lan**, **Outgoing Interface** to the SSID, and **Service** to allow connections from the Apple TV to the iOS device.

|                     |                           |   |
|---------------------|---------------------------|---|
| Incoming Interface  | lan (VLAN ID: 0)          | + |
| Source Address      | all                       | + |
| Source User(s)      | Click to add...           |   |
| Source Device Type  | Click to add...           |   |
| Outgoing Interface  | wireless (SSID: myWifi)   | + |
| Destination Address | all                       | + |
| Schedule            | always                    |   |
| Service             | AirPlay - Apple TV to iOS | + |
| Action              | ACCEPT                    |   |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Create a second policy allowing traffic from the iOS device to the Apple TV.

Set **Incoming Interface** to the SSID, **Outgoing Interface** to **lan**, and **Service** to allow connections from the iOS device to the Apple TV.

|                     |                           |   |
|---------------------|---------------------------|---|
| Incoming Interface  | wireless (SSID: myWifi)   | + |
| Source Address      | all                       | + |
| Source User(s)      | Click to add...           |   |
| Source Device Type  | Click to add...           |   |
| Outgoing Interface  | lan (VLAN ID: 0)          | + |
| Destination Address | all                       | + |
| Schedule            | always                    |   |
| Service             | AirPlay - iOS to Apple TV | + |
| Action              | ACCEPT                    |   |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

# 5. Results

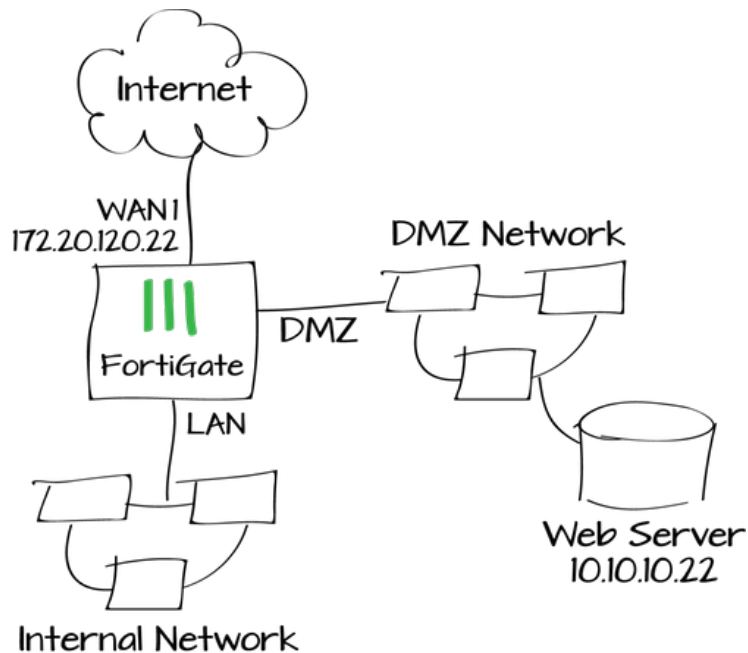
Use AirPlay to stream audio or video from an iOS device to the Apple TV.

Go to **Log & Report > Traffic Log > Multicast**. You will see traffic flowing between the two devices, using both multicast policies.

| #   | ▼ Date/Time | ▼ Source     | ▼ Destination | Sent / Received | ▼ Policy ID |
|-----|-------------|--------------|---------------|-----------------|-------------|
| ▶ 1 | 14:31:40    | 192.168.77.2 | 224.0.0.251   | 69 B / 0 B      | 1           |
| 2   | 14:31:40    | 10.10.20.3   | 224.0.0.251   | 118 B / 0 B     | 2           |
| 3   | 14:31:31    | 192.168.77.2 | 224.0.0.251   | 81 B / 0 B      | 1           |
| 4   | 14:31:30    | 10.10.20.3   | 224.0.0.251   | 59 B / 0 B      | 2           |
| 5   | 14:29:59    | 192.168.77.2 | 224.0.0.251   | 138 B / 0 B     | 1           |
| 6   | 14:29:58    | 10.10.20.3   | 224.0.0.251   | 118 B / 0 B     | 2           |
| 7   | 14:29:48    | 192.168.77.2 | 224.0.0.251   | 81 B / 0 B      | 1           |
| 8   | 14:29:48    | 10.10.20.3   | 224.0.0.251   | 59 B / 0 B      | 2           |
| 9   | 14:29:14    | 192.168.77.2 | 224.0.0.251   | 511 B / 0 B     | 1           |
| 10  | 14:29:05    | 192.168.77.2 | 224.0.0.251   | 4.90 KB / 0 B   | 1           |

For further reading, check out [Multicast forwarding](#) in the [FortiOS 5.2 Handbook](#).

# Protect a web server with DMZ



In the following example, you will protect a web server by connecting it using your FortiGate's DMZ network.

An internal to DMZ security policy with a virtual IP (VIP) allows internal users to access the web server using an internal IP address (10.10.10.22). A WAN-to-DMZ security policy also with a VIP hides the internal address, allowing external users to access the web server using a public IP address (172.20.120.22).

A video of this recipe is available [here](#).

## 1. Configuring the FortiGate's DMZ interface

Go to **System > Network > Interfaces**.  
Edit the **DMZ** interface.

The DMZ Network (from the term 'demilitarized zone') is a secure network connected to the FortiGate that only grants access if it has been explicitly allowed. Using the DMZ interface is recommended but not required.

For enhanced security, disable all **Administrative Access** options.

|                                       |   |  |  |
|---------------------------------------|---|--|--|
| Interface Name                        | dmz(00:09:0F:99:4B:E5)  |  |  |
| Alias                                 | <input type="text" value="DMZ server network"/>   |  |  |
| Link Status                           | Up  |  |  |
| Type                                  | Physical Interface  |  |  |
| Addressing mode                       | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer<br><input type="radio"/> Dedicated to Extension Device   |  |  |
| IP/Network Mask                       | <input type="text" value="10.10.10.1/255.255.255.0"/>   |  |  |
| Administrative Access                 | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP<br><input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access |  |  |
| DHCP Server                           | <input type="checkbox"/> Enable   |  |  |
| Security Mode                         | <input type="text" value="None"/>   |  |  |
| Device Management                     | <input type="checkbox"/> Detect and Identify Devices  |  |  |
| Listen for RADIUS Accounting Messages | <input type="checkbox"/>  |  |  |
| Secondary IP Address                  | <input type="checkbox"/>  |  |  |
| Comments                              | <input type="text" value=""/>   |  |  |
| Administrative Status                 | <input checked="" type="radio"/> Up <input type="radio"/> Down  |  |  |

## 2. Creating virtual IPs (VIPs)

Go to **Policy & Objects > Objects > Virtual IPs**. Create two virtual IPs: one for HTTP access and one for HTTPS access.

Each virtual IP has the same address, mapping from the public-facing interface to the DMZ interface. The difference is the port for each traffic type: port 80 for HTTP and port 443 for HTTPS.

|   |  |  |  |
|---|--|--|--|
| Name  | Web server http access   |  |  |
| Comments  | <input type="text" value=""/>  |  |  |
| Interface   | <input type="text" value="wan1"/>  |  |  |
| Type  | Static NAT   |  |  |
| <input type="checkbox"/> Source Address Filter      |  |  |  |
| External IP Address/Range                           | <input type="text" value="172.20.120.22"/> - <input type="text" value="172.20.120.22"/>                              |  |  |
| Mapped IP Address/Range                             | <input type="text" value="10.10.10.22"/> - <input type="text" value="10.10.10.22"/>                                  |  |  |
| <input checked="" type="checkbox"/> Port Forwarding |  |  |  |
| Protocol  | <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP |  |  |
| External Service Port                               | <input type="text" value="80"/> - <input type="text" value="80"/>  |  |  |
| Map to Port   | <input type="text" value="80"/> - <input type="text" value="80"/>  |  |  |

|   |  |                 |
|---|--|-----------------|
| Name  | Web server https access  |                 |
| Comments  | <div>0/255</div>   |                 |
| Interface   | wan1   |                 |
| Type  | Static NAT   |                 |
| <input type="checkbox"/> Source Address Filter      |  |                 |
| External IP Address/Range                           | 172.20.120.22  | - 172.20.120.22 |
| Mapped IP Address/Range                             | 10.10.10.22  | - 10.10.10.22   |
| <input checked="" type="checkbox"/> Port Forwarding |  |                 |
| Protocol  | <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP |                 |
| External Service Port                               | 443  | - 443           |
| Map to Port   | 443  | - 443           |

### 3. Creating security policies

Go to **Policy & Objects > Policy > IPv4**. Create a security policy to allow HTTP and HTTPS traffic from the Internet to the DMZ interface and the web server.

Do not enable NAT and, for testing purposes, enable logging for all sessions.

|                     |                          |     |
|---------------------|--------------------------|-----|
| Incoming Interface  | wan1                     | +   |
| Source Address      | all                      | +   |
| Source User(s)      | Click to add...          |     |
| Source Device Type  | Click to add...          |     |
| Outgoing Interface  | dmz (DMZ server network) | +   |
| Destination Address | Web server http access   | X + |
|                     | Web server https access  | X   |
| Schedule            | always                   |     |
| Service             | HTTP                     | X + |
|                     | HTTPS                    | X   |
| Action              | ACCEPT                   |     |

**Firewall / Network Options**

☐ NAT

Create a second security policy to allow HTTP and HTTPS traffic from the internal network to the DMZ interface and the web server.

Adding this policy allows traffic to pass directly from the internal interface to the DMZ interface.

Do not enable NAT and, for testing purposes, enable logging for all sessions.

Incoming Interface

Internal

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

dmz (DMZ server network)

Destination Address

all

Schedule

always

Service

HTTP

HTTPS

Action

ACCEPT

Firewall / Network Options

OFF

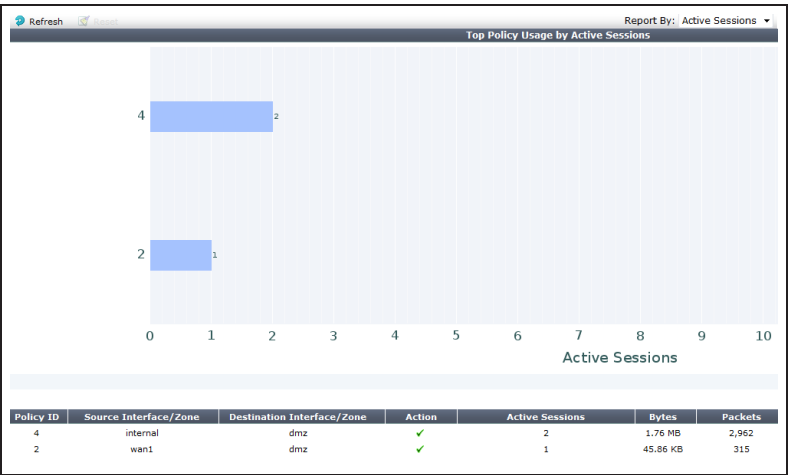
NAT

## 4. Results

External users can access the web server on the DMZ network from the Internet using its Internet address (in this example, `http://172.20.120.22` and `https://172.20.120.22`). Internal users can access the web server using its DMZ address (in this example, `http://10.10.10.22` and `https://10.10.10.22`). Internal users cannot access the web server using its Internet access because by default the FortiGate blocks hairpinning. For more information about hairpinning, see this [Knowledge Base article](#).

Go to **Policy & Objects > Monitor > Policy Monitor**.

Use the policy monitor to verify that traffic from the Internet and from the internal network is allowed to access the web server. This verifies that the policies are configured correctly.



Go to **Log & Report > Traffic Log > Forward Traffic**.

The traffic log shows sessions from the internal network and from the Internet accessing the web server on the DMZ network.

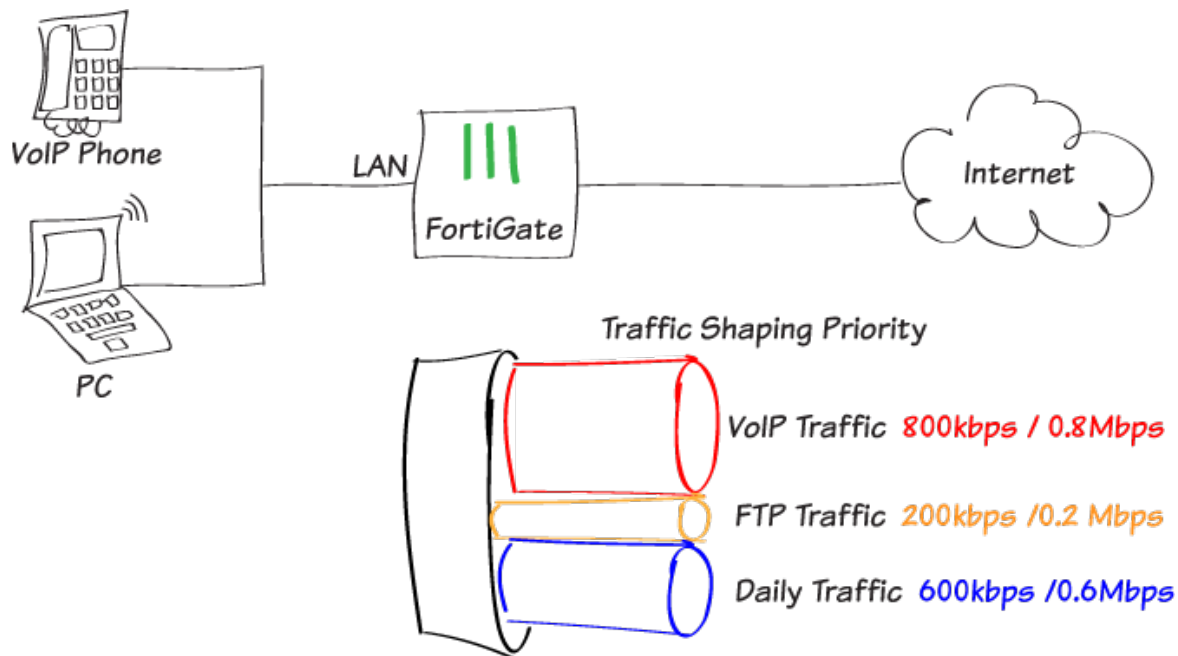
| Refresh Download Raw Log |                |               |               |                 |             |                   |           | Log location: Disk |  |
|--------------------------|----------------|---------------|---------------|-----------------|-------------|-------------------|-----------|--------------------|--|
| #                        | Date/Time      | Src Interface | Dst Interface | Src             | Dst         | Sent / Received   | Policy ID | Service            |  |
| 3                        | 3 seconds ago  | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 48 B / 40 B       | 4         | HTTP               |  |
| 4                        | 3 seconds ago  | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 0 B / 0 B         | 4         | HTTP               |  |
| 5                        | 4 seconds ago  | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 0 B / 0 B         | 4         | HTTP               |  |
| 6                        | 31 seconds ago | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 1.21 KB / 1.59 KB | 4         | HTTPS              |  |
| 7                        | 31 seconds ago | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 1.16 KB / 1.63 KB | 4         | HTTPS              |  |
| 8                        | 33 seconds ago | internal      | dmz           | 192.168.100.110 | 10.10.10.22 | 839 B / 1.40 KB   | 4         | HTTPS              |  |

| Refresh Download Raw Log |                |               |               |                |               |             |           | Log location: Disk |  |
|--------------------------|----------------|---------------|---------------|----------------|---------------|-------------|-----------|--------------------|--|
| #                        | Date/Time      | Src Interface | Dst Interface | Src            | Dst           | Dst NAT IP  | Policy ID | Service            |  |
| 1                        | 4 seconds ago  | wan1          | dmz           | 172.20.120.21  | 172.20.120.22 | 10.10.10.22 | 2         | HTTP               |  |
| 2                        | 57 seconds ago | wan1          | dmz           | 172.20.120.123 | 172.20.120.22 | 10.10.10.22 | 2         | HTTPS              |  |
| 3                        | 1 minute ago   | wan1          | dmz           | 172.20.120.123 | 172.20.120.22 | 10.10.10.22 | 2         | HTTPS              |  |

For further reading, check out **Firewall** in the **FortiOS 5.2 Handbook**.



# Traffic shaping for VoIP



The quality of VoIP phone calls through a firewall often suffers when the firewall is busy and the amount of bandwidth available for the VoIP traffic fluctuates. This can be irritating, leading to unpredictable results and caller frustration. This recipe describes how to add traffic shaping to guarantee that enough bandwidth is available for VoIP traffic, regardless of any other activity on the network.

To achieve high quality real-time voice transmissions, VoIP traffic requires priority over other types of traffic, minimal packet loss, and jitter buffers. You will limit bandwidth consuming services, like FTP, while providing a consistent bandwidth for day-to-day email and web-based traffic. First, you will customize three existing traffic shapers—high priority, medium priority, and low priority—and then create a separate security policy for each service type.

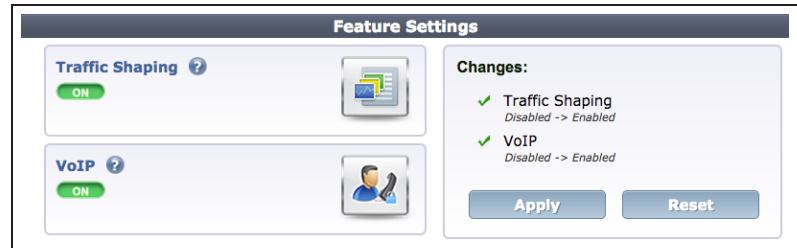
*Before you apply QoS measures, ensure you have enough network bandwidth to support real-time voice traffic.*

A video of this recipe is available [here](#).

## 1. Enabling Traffic Shaping and VoIP features

Go to **System > Config > Features** and click the **Show More** button to view additional features. If necessary, select **ON** to enable both **Traffic Shaping** and **VoIP**. Apply your changes.

*Traffic shaping rules and VoIP profiles can now be applied to firewall policies.*



The screenshot shows the 'Feature Settings' window. On the left, there are two sections: 'Traffic Shaping' with a status of 'ON' and a help icon, and 'VoIP' also with a status of 'ON' and a help icon. On the right, under 'Changes:', there are two green checkmarks: 'Traffic Shaping Disabled -> Enabled' and 'VoIP Disabled -> Enabled'. At the bottom right are 'Apply' and 'Reset' buttons.

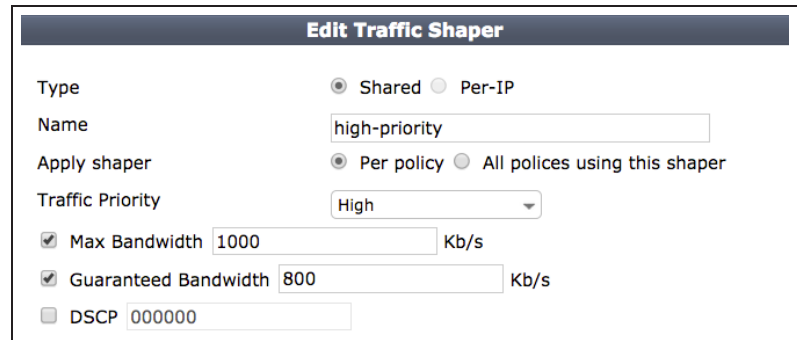
## 2. Configuring a high priority VoIP traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **high-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **Per Policy**.

*Select **Per Policy** when you want each security policy for day-to-day business traffic to have the same distribution of bandwidth, regardless of the number of policies using the shaper. In this example, 800kb/s (0.8Mbps) each.*

Set **Traffic Priority** to **High**. Select **Max Bandwidth** and enter 1000 kb/s (1 Mbps). Select **Guaranteed Bandwidth** and enter 800 kb/s (0.8 Mbps).



The screenshot shows the 'Edit Traffic Shaper' window for a shaper named 'high-priority'. The 'Type' is set to 'Shared' (radio button selected). The 'Name' field contains 'high-priority'. The 'Apply shaper' is set to 'Per policy' (radio button selected). The 'Traffic Priority' is set to 'High' (dropdown menu). There are three checked options: 'Max Bandwidth' set to 1000 Kb/s, 'Guaranteed Bandwidth' set to 800 Kb/s, and 'DSCP' set to 000000.

### 3. Configuring a low priority FTP traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **low-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **All policies using this shaper**.

*Select **All policies using this shaper** to ensure that **all** policies using your shaper will be restricted to share a set amount of bandwidth. In this example, 200kb/s (0.2 Mbps) total.*

Set **Traffic Priority** to **Low**.

*If you are creating a new traffic shaper, the **Traffic Priority** is set to **High** by default. A failure to set different shaper priorities will result in a lack of prioritized traffic.*

Set **Max Bandwidth** and **Guaranteed Bandwidth** to 200 kb/s (0.2 Mbps).

*Setting a low maximum bandwidth will prevent sudden spikes in traffic caused by large FTP file uploads and downloads.*

Edit Traffic Shaper

Type

☒ Shared ☐ Per-IP

Name

low-priority

Apply shaper

☐ Per policy ☒ All policies using this shaper

Traffic Priority

Low

☒ Max Bandwidth

200

Kb/s

☒ Guaranteed Bandwidth

200

Kb/s

☐ DSCP

000000

## 4. Configuring a medium priority daily traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **medium-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **Per Policy**. Select **Max Bandwidth** and enter 600 kb/s (0.6 Mbps). Set **Traffic Priority** to **Medium**. Select **Guaranteed Bandwidth** and enter 600 kb/s (0.6 Mbps).

*This shaper should be set to a moderate value and set to **per policy** so that day-to-day traffic has the same distribution of bandwidth.*

**Edit Traffic Shaper**

|  |   |
|--|---|
| Type   | <input checked="" type="radio"/> Shared <input type="radio"/> Per-IP                            |
| Name   | <input type="text" value="medium-priority"/>  |
| Apply shaper   | <input checked="" type="radio"/> Per policy <input type="radio"/> All polices using this shaper |
| Traffic Priority   | <input type="text" value="Medium"/>   |
| <input checked="" type="checkbox"/> Max Bandwidth        | <input type="text" value="600"/> Kb/s   |
| <input checked="" type="checkbox"/> Guaranteed Bandwidth | <input type="text" value="600"/> Kb/s   |
| <input type="checkbox"/> DSCP                            | <input type="text" value="000000"/>   |

# 5. Applying each shaper to a device-based policy

Go to **Policy & Objects > Policy > IPv4** and create a new security policy for SIP traffic.

Enable **Shared Shaper** and **Reverse Shaper** and select **high-priority**.

*Make sure that you include a **Reverse Shaper** so that return traffic for a VoIP call has the same guaranteed bandwidth as an outgoing call.*

For **Logging Options**, select **All Sessions** for testing purposes.

New Policy

Incoming Interface

lan (VLAN ID: 0)

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1 (external)

+

Destination Address

all

+

Schedule

always

Service

SIP

+

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

ON

VoIP

default

ON

SSL/SSH Inspection

certificate-inspection

Traffic Shaping

ON

Shared Shaper

high-priority

ON

Reverse Shaper

high-priority

OFF

Per-IP Shaper

Click to set...

Logging Options

ON

Log Allowed Traffic

Security Events

All Sessions

Go to **Policy & Objects > Policy > IPv4** and create a security policy for FTP traffic.

New Policy

Incoming Interface

lan (VLAN ID: 0)

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1 (external)

Destination Address

all

Schedule

always

Service

FTP

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

OFF

VoIP

default

OFF

SSL/SSH Inspection

certificate-inspection

Traffic Shaping

ON

Shared Shaper

low-priority

ON

Reverse Shaper

low-priority

OFF

Per-IP Shaper

Click to set...

Logging Options

ON

Log Allowed Traffic

Security Events

All Sessions

Go to **Policy & Objects > Policy > IPv4** and create a security policy for daily web-based, email traffic, and other traffic.

*You can also edit your existing general access security policy.*

Edit Policy

Incoming Interface

lan (VLAN ID: 0)

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1 (external)

+

Destination Address

all

+

Schedule

always

Service

ALL

+

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

OFF

VoIP

default

OFF

SSL/SSH Inspection

certificate-inspection

Traffic Shaping

ON

Shared Shaper

medium-priority

ON

Reverse Shaper

medium-priority

OFF

Per-IP Shaper

Click to set...

Logging Options

ON

Log Allowed Traffic

Security Events

All Sessions

Arrange your policies are in the following order:

*Click on the far left of the column you want to move and drag it up or down to arrange it.*

1.

High-priority (SIP/VoIP traffic)
2.

Low-priority (FTP traffic)
3.

Medium-priority (Day-to-day traffic)

*More specific restrictive policies, like the SIP and FTP policies, should always be placed at the top of the list, above the unrestricted general access policy that allows "all".*

Create New Edit Delete

Section View Global View

Search

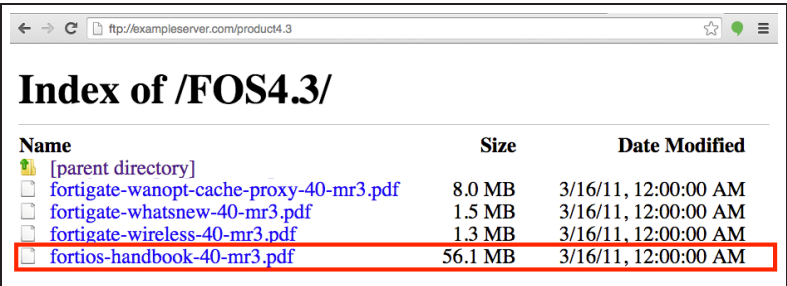
| Seq.# | From | To              | Source | Destination | Traffic Shaper                     | Service | Action |
|-------|------|-----------------|--------|-------------|------------------------------------|---------|--------|
| 1     | lan  | wan1 (external) | all    | all         | high-priority<br>high-priority     | SIP     | ACCEPT |
| 2     | lan  | wan1 (external) | all    | all         | low-priority<br>low-priority       | FTP     | ACCEPT |
| 3     | lan  | wan1 (external) | all    | all         | medium-priority<br>medium-priority | ALL     | ACCEPT |
| 4     | any  | any             | all    | all         |                                    | ALL     | DENY   |

## 6. Results

Browse the Internet using a PC on your internal network to generate daily web traffic. Then, generate FTP traffic.

*In this example, a 56.1 MB file was downloaded from an FTP server.*

The FTP download or upload should occur slowly.



| Name                                    | Size    | Date Modified        |
|---|---------|----------------------|
| [parent directory]                      |         |                      |
| fortigate-wanopt-cache-proxy-40-mr3.pdf | 8.0 MB  | 3/16/11, 12:00:00 AM |
| fortigate-whatsnew-40-mr3.pdf           | 1.5 MB  | 3/16/11, 12:00:00 AM |
| fortigate-wireless-40-mr3.pdf           | 1.3 MB  | 3/16/11, 12:00:00 AM |
| fortios-handbook-40-mr3.pdf             | 56.1 MB | 3/16/11, 12:00:00 AM |

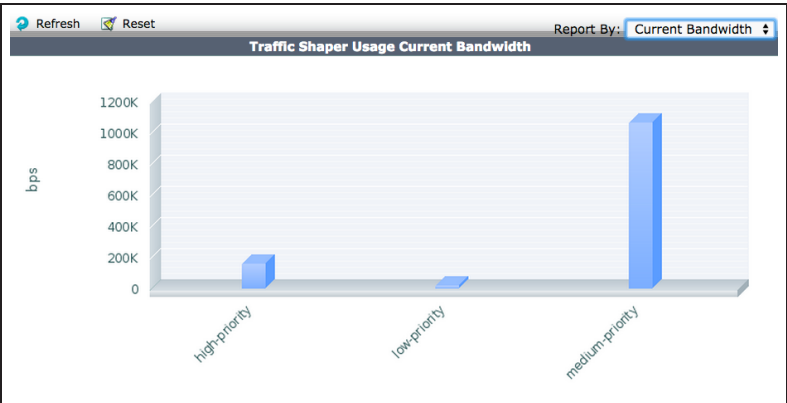
Finally, generate SIP traffic.

*In this example, SIP traffic was generated by placing a call with a VoIP FortiFone connected to the internal interface of the FortiGate.*

Go to **Policy & Objects > Monitor > Traffic Shaper Monitor** and report by the **Current Bandwidth**. You can see how much of your current bandwidth is being used by active traffic shapers. If the standard traffic volume is high enough, it will top out at the maximum bandwidth defined by each shaper.

*In the screenshot, the SIP traffic is only using a small part of the allocated bandwidth.*

You will have normal voice quality on your VoIP call, even with daily traffic and FTP downloads running.





Go to **Log & Report > Log & Archive Access > Traffic Log** and filter the **Service** by **SIP** to see your VoIP traffic. Select an individual log message to view the shaper name in the **Sent Shaper Name** field.

| # | Service | Date/Time   | Source     | Device            | Destination    | Application Name |  |
|---|---------|-------------|------------|-------------------|----------------|------------------|--|
| 1 | SIP     | 03-18 16:06 | 10.10.13.4 | b4:0e:dc:b9:bf:5a | 172.20.190.254 | unknown-12       |  |
| 2 | SIP     | 03-18 16:01 | 10.10.13.4 | b4:0e:dc:b9:bf:5a | 172.20.190.254 | unknown-12       |  |
| 3 | SIP     | 03-18 15:45 | 10.10.13.4 | b4:0e:dc:b9:bf:5a | 172.20.190.254 | unknown-12       |  |

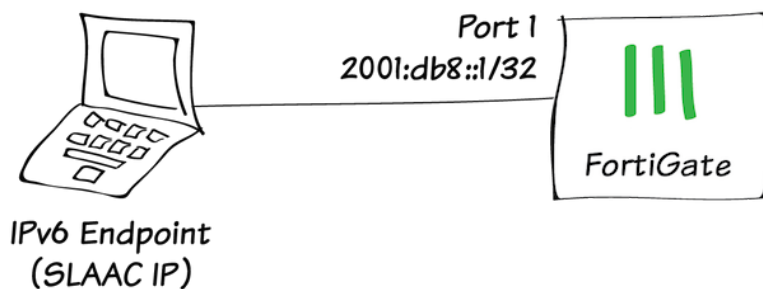
1 / 1

Total: 3

|                      |                                      |                               |                   |
|----------------------|--------------------------------------|-------------------------------|-------------------|
| #                    | 1                                    | Action                        | accept            |
| Application ID       | 12                                   | Application Name              | unknown-12        |
| Date/Time            | 03-18 16:06                          | Destination                   | 172.20.190.254    |
| Destination Country  | Reserved                             | Device                        | b4:0e:dc:b9:bf:5a |
| Device Type          | Error                                | Dst Interface                 | unknown-0         |
| Dst Port             | 5060                                 | Duration                      | 196               |
| Level                | 12345                                | Log ID                        | 13                |
| Master Src MAC       | b4:0e:dc:b9:bf:5a                    | Policy ID                     | 2                 |
| Policy UUID          | 76642b46-b856-51e4-c820-7d4664492ef6 | Protocol                      | udp               |
| Protocol Number      | 17                                   | Received                      | 0                 |
| Received Packets     | 0                                    | Received Shaper Bytes Dropped | 0                 |
| Received Shaper Name | high-priority-VoIP                   | Sent                          | 4776              |
| Sent Packets         | 8                                    | Sent Shaper Bytes Dropped     | 0                 |
| Sent Shaper Name     | high-priority-VoIP                   | Sequence Number               | 74777             |
| Service              | SIP                                  | Source                        | 10.10.13.4        |
| Source Country       | Reserved                             | Src Interface                 | unknown-0         |
| Src Port             | 5060                                 | Sub Type                      | forward           |
| Timestamp            | 3/18/2015, 4:06:24 PM                | Tran Display                  | noop              |
| Virtual Domain       | root                                 |                               |                   |

For further reading, check out [Traffic Shaping](#) in the [FortiOS 5.2 Handbook](#).

# Creating an IPv6 interface using SLAAC



In this example you will configure your FortiGate to use Stateless Address Auto Configuration (SLAAC) to assign IPv6 addresses to IPv6-enabled devices on your internal network.

The IPv6 address block used in this recipe (2001:db8::/32) is reserved for documentation purposes and will not work on your network. If you're not sure how to determine the correct IPv6 address for your environment, refer to the [FortiOS IPv6 Handbook Chapter](#).

## 1. Enabling IPv6

Go to **System > Config > Features** and make sure that **IPv6** is turned **ON**.



## 2. Configuring a FortiGate interface for IPv6

Go to **System > Network > Interfaces** and edit the interface connected to your internal network (in the example, port1).

Set the **IPv6 Addressing mode** to **Manual** and enter the **IPv6 Address/Prefix** for the interface (in this example, 2001:db8::1/32).

|                      |  |
|----------------------|--|
| Interface Name       | port1(00:09:0F:BC:0E:68)   |
| Alias                | <input type="text"/>   |
| Link Status          | Up   |
| Type                 | Physical Interface   |
| Addressing mode      | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> Dedicated to Extension Device |
| IP/Network Mask      | <input type="text" value="0.0.0.0/0.0.0.0"/>   |
| IPv6 Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP   |
| IPv6 Address/Prefix  | <input type="text" value="2001:db8::1/32"/>  |

The interface can have both IPv4 and IPv6 addressing. This example only includes IPv6 addressing.

Enter this CLI command to add the router advertisements and specific IPv6 prefixes required to configure SLAAC on the interface.

```
config system interface
edit port1
config ipv6
set ip6-address 2001:db8::1/32
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8::/32
set autonomous-flag enable
set onlink-flag enable
end
end
end
```

The `set ip6-address` option is not required since you already added an IPv6 address to the interface from the GUI. But its included in the example to show the complete CLI configuration.

### 3. Adding IPv6 firewall addresses

Go to **Policy & Objects > Objects > Addresses > Create New**.

Add an IPv6 firewall address that matches the IPv6 address added to the port1 interface.

|              |   |
|--------------|---|
| Category     | <input type="radio"/> Address <input checked="" type="radio"/> IPv6 Address |
| Name         | <input type="text" value="port1-IPv6-address"/>                             |
| Type         | <input type="text" value="Subnet"/>   |
| IPv6 Address | <input type="text" value="2001:db8::1/32"/>                                 |
| Visibility   | <input checked="" type="checkbox"/>   |
| Comments     | <input type="text" value="matches the port1 IPv6 address"/> 30/255          |

### 4. ‘Bouncing’ the IPv6 interface

You can now ‘bounce’ the port1 interface (bring the interface down and then back up). Go to **System > Network > Interfaces**, edit the port1 interface and set the **Administrative Access** to **Down**. Select **OK**, then edit the interface again and set the **Administrative Access** back to **Up**. This causes a router advertisement using the Neighbor Discovery Protocol, which performs address autoconfiguration and determines the reachability of neighboring nodes.

Alternatively, you can reboot the FortiGate or wait for the next router advertisement.

### 5. Results

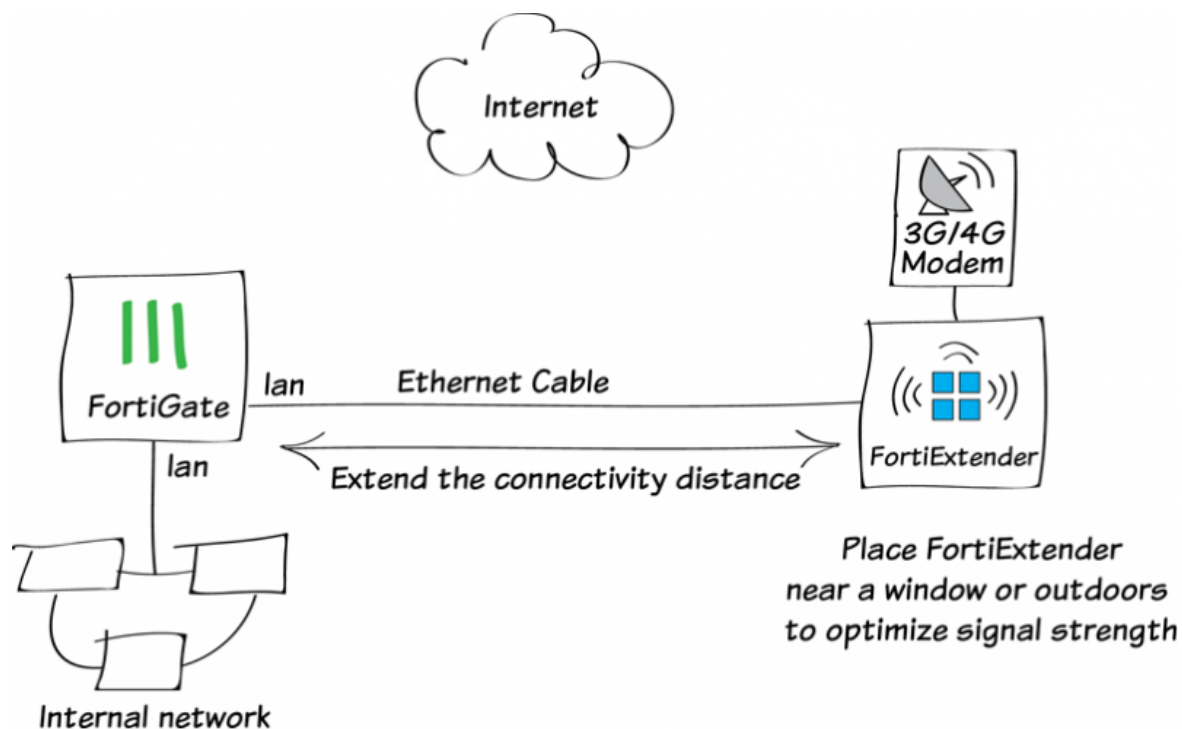
Connect a computer to the port1 interface. Configure the computer to get an IPv6 address automatically. Then, from a command prompt or terminal session enter the command `ipconfig` to view the computer’s IP configuration.

IPv6 Address.....: 2001:db8::44d2:ed21:9733:9245

You should see that an IPv6 address has been assigned with the prefix advertised on the port1 interface.

For further reading, check out **IPv6** in the **FortiOS 5.2 Handbook**.

# FortiExtender installation



This example shows how to set an internet connection using a 3G/4G modem and a FortiExtender. A FortiExtender is used when the FortiGate unit is located in an area without 3G/4G network coverage, the FortiExtender can be placed near a window or outdoors.

For information about the compatibility of FortiExtender and various modems, see the [FortiGate and FortiExtender Modem Compatibility Matrix](#).

## 1. Installing the 3G/4G modem in the FortiExtender

Remove the housing cover of the FortiExtender and use the provided USB extension cable to connect your 3G/4G modem to the device.

For more information on installing the 3G/4G modem, see the QuickStart Guide.



## 2. Connecting the FortiExtender

Use an Ethernet cable to connect the FortiExtender to the **lan** interface of a FortiGate unit.

Once connected, FortiGate can control FortiExtender and modem.

Enable FortiExtender in the FortiGate's CLI.

CAPWAP service must be enabled on the port to which FortiExtender is connected, **lan** interface in this example.

```
config system global
    set fortiextender enable
    set wireless-controller enable
end

config system interface
    edit lan
        append allowaccess capwap
    end
end
```

Once enabled, it appears as a virtual WAN interface in the FortiGate, such as **fext-wan1**. Go to **System > Network > Interface** to verify **fext-wan1** interface.




|                  |   |
|------------------|---|
| <b>lan</b>       |  <b>Hardware Switch (16)</b> |
| <b>fext-wan1</b> |  <b>FortiExtender</b>        |

### 3. Configuring the FortiExtender

Go to **System > Network > FortiExtender** and authorize the FortiExtender.

Once authorized, you can see the status of the FortiExtender.

| Primary               |  |
|-----------------------|--|
| Serial Number         | FX100B3X14000077   |
| Administrative Status |  Deauthorized [ <a href="#">Authorize</a> ] |

| Primary  |  |
|--|--|
| Serial Number  | FX100B3X14000077   |
| Model  | FX100B   |
| Administrative Status  |  Authorized [ <a href="#">Deauthorize</a> ] |
| Link Status  |  Up [ <a href="#">Details</a> ]             |
| MAC Address  | 8:5b:e:5b:71:d0  |
| IP Address   | <a href="#">192.168.1.100</a>  |
| OS Version   | FX100B-v1.0-build024 [ <a href="#">Upgrade</a> ]   |
| Network  |  N/A  |
| Data Usage   |  |
| Current Usage  |  |
| <div><div></div></div> 653.22 KB of 653.22 KB (100.00%)        |  |
| Last Month Usage   |  |
| <div><div></div></div> 0 B of 0 B (0.00%)                      |  |
| <div><div>Configure Settings</div><div>Diagnostics</div></div> |  |

## 4. Modem settings

The FortiExtender unit allows for two modes of operation for the modem; On Demand and Always Connect.

Go to **System > Network > FortiExtender** and click on **Configuring Settings**.

Select **Always Connect** for **Dial Mode** and keep other settings to default.

**Settings for FX100B3X14000077 - Primary**

▼ **Modem Settings**

Dial Mode

☐ On Demand ☒ Always Connect

Redial Limit

0

Quota Limit (MB)

0

▼ **PPP Authentication**

Username

Password

••••••••

Authentication Protocol

auto

▶ **General**

▶ **GSM / LTE**

▶ **CDMA**

## 5. Configuring the FortiGate

Go to **Router > Static > Static Routes** and add new route through **fext-wan1** interface.

|                     |  |
|---------------------|--|
| Destination IP/Mask | <input type="text" value="0.0.0.0/0.0.0.0"/>       |
| Device              | <input type="text" value="fext-wan1"/>             |
| Gateway             | <input type="text" value="0.0.0.0"/>               |
| Distance            | <input type="text" value="5"/> (1-255, Default=10) |
| Priority            | <input type="text" value="0"/> (0-4294967295)      |
| Comments            | <input type="text" value="Write a comment..."/>    |



Go to **Policy & Objects > Policy > IPv4** and create a new security policy allowing traffic from **lan** interface to **fext-wan1** interface.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | lan             |
| Source Address      | all             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | fext-wan1       |
| Destination Address | all             |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

**Firewall / Network Options**

☒ NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

☐ Web Cache

☐ WAN Optimization

6. Results

Browse the Internet and go to **Policy & Objects > Policy > IPv4** to verify the Count.

| Seq.#                      | ID | Source | Destination | Count                       |
|----------------------------|----|--------|-------------|-----------------------------|
| ike-bgp-fgt1 - lan (1 - 1) |    |        |             |                             |
| 4                          | 8  | all    | all         | 0 Packets / 0 B             |
| lan - fext-wan1 (2 - 2)    |    |        |             |                             |
| 6                          | 9  | all    | all         | 8,441 Packets / 2.19 MB     |
| lan - ike-bgp-fgt1 (3 - 3) |    |        |             |                             |
| 3                          | 7  | all    | all         | 0 Packets / 0 B             |
| lan - wan1 (4 - 4)         |    |        |             |                             |
| 5                          | 10 | all    | all         | 974,394 Packets / 664.12 MB |

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic flowing from **lan** interface to **fext-wan1** interface.

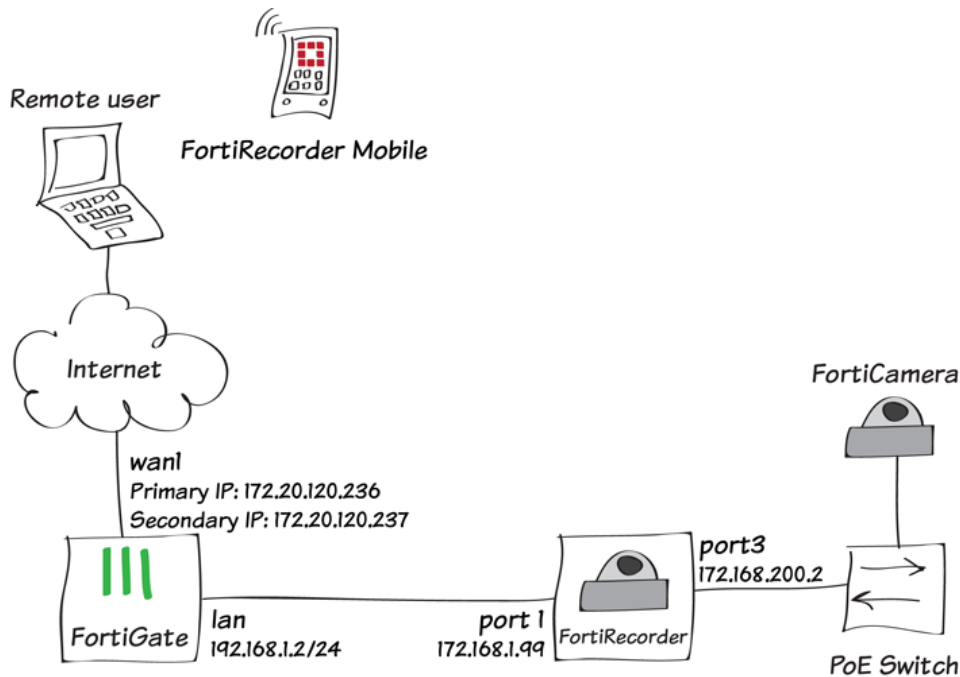
| ▼ Date... | ▼ Policy ... | ▼ Src Interface | ▼ Dst Interface |
|-----------|--------------|-----------------|-----------------|
| 15:38:03  | 9            | lan             | fext-wan1       |
| 15:37:47  | 9            | lan             | fext-wan1       |
| 15:37:43  | 9            | lan             | fext-wan1       |
| 15:37:39  | 9            | lan             | fext-wan1       |
| 15:37:35  | 9            | lan             | fext-wan1       |
| 15:37:31  | 9            | lan             | fext-wan1       |
| 15:37:19  | 9            | lan             | fext-wan1       |
| 15:37:07  | 9            | lan             | fext-wan1       |
| 15:36:59  | 9            | lan             | fext-wan1       |
| 15:36:55  | 9            | lan             | fext-wan1       |
| 15:36:31  | 9            | lan             | fext-wan1       |
| 15:36:27  | 9            | lan             | fext-wan1       |

Select an entry for details.

|                 |             |                 |  |
|-----------------|-------------|-----------------|--|
| Action          | ip-conn     | Date/Time       | 15:35:51 (1405006551)  |
| Destination     | 10.10.80.25 | Dst Interface   | fext-wan1  |
| Dst Port        | 161         | Level           | warning <div><div></div><div></div><div></div><div></div><div></div></div> |
| Log ID          | 11          | Policy ID       | 9  |
| Security Events |             | Sent / Received | N/A / N/A  |
| Sequence Number | 10016       | Source          | 192.168.1.101  |
| Src Interface   | lan         | Src Port        | 56442  |
| Sub Type        | forward     | Threat          | 262144   |
| Threat Score    | 1375731722  | Timestamp       | 7/10/2014, 3:35:51 PM  |
| Virtual Domain  | root        |                 |  |

For further reading, check out [FortiExtender](#) in the [FortiOS 5.2 Handbook](#).

# Remotely accessing FortiRecorder through a FortiGate



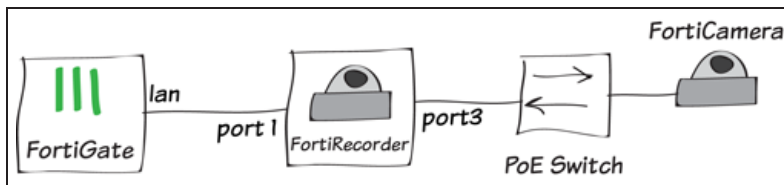
In this recipe, you set up a FortiGate with a secondary IP to provide remote access to a FortiRecorder. This allows you to securely view live FortiCamera video feeds over the Internet, using either the FortiRecorder GUI, FortiRecorder Mobile, or FortiRecorder Central.

This recipe employs a secondary IP and two port forwarding virtual IPs to forward HTTPS and Real Time Streaming Protocol (RTSP) packets from the Internet to the FortiRecorder. To use a secondary IP address you must have a second Internet IP address for your FortiRecorder. Instead of adding this IP address to the FortiRecorder, you add it to your FortiGate and forward traffic for the FortiRecorder IP address through the FortiGate.

## 1. Connect the hardware

Connect your devices as shown in the diagram.

In this example, the FortiCamera connects to a PoE switch, which is then connected to **port3** on the FortiRecorder. The FortiRecorder's **port1** connects to the FortiGate **lan** interface.



## 2. Configuring the FortiRecorder and FortiCamera

On the FortiRecorder, go to **System > Network > Interface** and edit **port1**. Set a manual **IP/Netmask** for the interface that is on the same subnet as the FortiGate **lan** interface (in the example, *192.168.1.99*).

Set **Access** to allow HTTPS and any other protocols you require. If you are using FortiRecorder Central, you must enable **FRC-Central**.

Interface name: port1 (8c:89:a5:5f:a5:a5)

☐ Discover cameras on this port

**Addressing Mode**

☒ Manual

IP/Netmask: 192.168.1.99 / 24

IPv6/Netmask: :: / 0

☐ DHCP

☐ Retrieve default gateway and DNS from server

☐ Connect to server

**Access**

☒ HTTPS ☒ PING ☐ HTTP ☒ FRC-Central

☒ SSH ☐ SNMP ☐ TELNET

**MTU**

☐ Override default MTU value (1500)

1500 (bytes)

**Administrative status** ☒ Up ☐ Down

Edit **port3**. Make sure that **Discover cameras on this port** is enabled. Set a manual **IP/Netmask** for the interface.

Interface name: port3 (8c:89:a5:5f:a5:a7)

☒ Discover cameras on this port

**Addressing Mode**

☒ Manual

IP/Netmask: 192.168.200.2 / 24

IPv6/Netmask: :: / 0

☐ DHCP

☐ Retrieve default gateway and DNS from server

☐ Connect to server

Go to **System > Network > DHCP** and create a new DHCP server. Set **Interface** to **port3** and **Gateway** to port3's IP address (in the example, *192.168.200.2*).

Create a new **DHCP IP Range** that is on the same subnet as port3.

ID: 0

Enable DHCP server: ☒

Interface: port3

Gateway: 192.168.200.2

DNS options: Default

DNS server 1: 0.0.0.0

DNS server 2: 0.0.0.0

Domain:

Netmask: 255.255.255.0

**Auto Config Setting**

Lease time (Seconds): 604800

Conflicted IP timeout (Seconds): 1800

**DHCP IP Range**

New... Edit... Delete

| Start         | End           |
|---------------|---------------|
| 192.168.2.100 | 192.168.2.200 |

Go to **System > Network > Routing**. Add a default route that uses the IP address of the FortiGate's lan interface (in the example, 192.168.1.2). Set **Interface** to **port1**.

Destination IP/netmask: 0.0.0.0 / 0

Interface: port1

Gateway: 192.168.1.2

Go to **Camera > Configuration > Camera**. Click on **Force Discover** to have connected cameras displayed.

| Camera Name   | Vendor   | Model    | Version | Location | Address         | MAC Address       | Profile | Status         |
|---------------|----------|----------|---------|----------|-----------------|-------------------|---------|----------------|
| FCM-MB13-605a | Fortinet | FCM-MB13 |         |          | 192.168.200.101 | 00:22:14:ce:60:5a |         | Not Configured |

The FortiCamera will appear on the list, with the **Status** column displayed as **Not Configured**.

Select the FortiCamera and select **Configure**. Set the unit's **Name** and **Location**, and **Profile**, as well as any other required configuration settings.

*If you do not have any profiles already created, you will have to configure one. For more information, see the [FortiRecorder 2.0.0 Administration guide](#).*

Enabled: ☒

Name: big-sister

Location: everywhere

Vendor: Fortinet Camera detail

Model: FCM-MB13

Address mode: Wired

Address: 192.168.200.101 Port: 443

Transport type: UDP Port: 554

Profile: Motion-detect New... Edit...

### 3. Adding a secondary IP to the FortiGate

From the FortiGate GUI, go to **System > Network > Interfaces** and edit your Internet-facing interface.

Enable **Secondary IP Address** and create a new **IP/Network Mask** for the interface.

Secondary IP Address

IP/Network Mask 172.20.120.237/255.255.255.0

Administrative Access

☐ HTTPS ☐ PING

☐ HTTP ☐ FMG-Access

☐ CAPWAP

☐ SSH ☐ SNMP

☐ TELNET

Adding a secondary IP address allows the FortiGate and the network to see two IP addresses, the primary and the secondary, that terminate at the interface.

In this example, the primary IP address is used to connect to the FortiGate, while the secondary IP will be used to connect to the FortiRecorder.

Interface Name: wan1(00:09:0F:B0:EB:EA)  
Alias:   
Link Status: Up  
Type: Physical Interface

Addressing mode: ☒ Manual ☐ DHCP ☐ PPPoE ☐ Dedicated to Extension Device  
IP/Network Mask: 172.20.120.236/255.255.255.0  
IPv6 Addressing mode: ☒ Manual ☐ DHCP  
IPv6 Address/Prefix:

Administrative Access: ☒ HTTPS ☒ PING ☒ HTTP ☒ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ FCT-Access  
☒ Auto IPsec Request

IPv6 Administrative Access: ☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP

DHCP Server: ☐ Enable

Security Mode:

Device Management: ☐ Detect and Identify Devices

Enable Explicit Web Proxy: ☐  
Listen for RADIUS Accounting Messages: ☒  
Secondary IP Address: ☒

| IP/Network Mask              | Administrative Access |
|------------------------------|-----------------------|
| 172.20.120.237/255.255.255.0 |                       |

## 4. Creating virtual IPs

From the FortiGate GUI, go to **Policy & Objects > Objects > Virtual IPs**. Create the two virtual IPs: one for HTTPS traffic and one for RTSP traffic.

For both virtual IPs, set **External Interface** to your Internet-facing interface, **External IP Address/Range** to the secondary IP of that interface (in the example, 172.20.120.237) and the **Mapped IP Address/Range** to the IP of port1 on the FortiRecorder unit (in the example, 192.168.1.99).

Enable **Port Forwarding** and use the standard port for each protocol. HTTPS uses TCP port 443 and RTSP uses TCP port 554.

VIP Type: ☒ IPv4 VIP ☐ IPv6 VIP ☐ NAT46 VIP ☐ NAT64 VIP  
Name: FortiRecorder\_HTTPS  
Comments:  0/255  
Interface: wan1  
Type: Static NAT  
☐ Source Address Filter  
External IP Address/Range: 172.20.120.237 - 172.20.120.237  
Mapped IP Address/Range: 192.168.1.99 - 192.168.1.99  
☒ Port Forwarding  
Protocol: ☒ TCP ☐ UDP ☐ SCTP ☐ ICMP  
External Service Port: 443 - 443  
Map to Port: 443 - 443

|   |  |  |
|---|--|--|
| VIP Type  | <input checked="" type="radio"/> IPv4 VIP <input type="radio"/> IPv6 VIP <input type="radio"/> NAT46 VIP <input type="radio"/> NAT64 VIP |  |
| Name  | FortiRecorder_RTSP   |  |
| Comments  | <div></div> 0/255  |  |
| Interface   | wan1   |  |
| Type  | Static NAT   |  |
| <input type="checkbox"/> Source Address Filter      |  |  |
| External IP Address/Range                           | 172.20.120.237 - 172.20.120.237  |  |
| Mapped IP Address/Range                             | 192.168.1.99 - 192.168.1.99  |  |
| <input checked="" type="checkbox"/> Port Forwarding |  |  |
| Protocol  | <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP                     |  |
| External Service Port                               | 554 - 554  |  |
| Map to Port   | 554 - 554  |  |

If you are using FortiRecorder Central, you must create a third virtual IP to allow TCP port 8550.

|   |  |  |
|---|--|--|
| VIP Type  | <input checked="" type="radio"/> IPv4 VIP <input type="radio"/> IPv6 VIP <input type="radio"/> NAT46 VIP <input type="radio"/> NAT64 VIP |  |
| Name  | FortiRecorder_Central  |  |
| Comments  | <div></div> 0/255  |  |
| Interface   | wan1   |  |
| Type  | Static NAT   |  |
| <input type="checkbox"/> Source Address Filter      |  |  |
| External IP Address/Range                           | 172.20.120.237 - 172.20.120.237  |  |
| Mapped IP Address/Range                             | 192.168.1.99 - 192.168.1.99  |  |
| <input checked="" type="checkbox"/> Port Forwarding |  |  |
| Protocol  | <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP                     |  |
| External Service Port                               | 8550 - 8550  |  |
| Map to Port   | 8550 - 8550  |  |

## 5. Creating a security policy to access to the FortiRecorder

Go to **Policy & Object > Policy > IPv4** and create a new policy that allows access to the FortiRecorder from the Internet.

Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to lan, and **Destination Address** to the new virtual IPs.

|   |                       |   |
|---|-----------------------|---|
| Incoming Interface  | wan1                  | + |
| Source Address  | all                   | + |
| Source User(s)  | Click to add...       |   |
| Source Device Type  | Click to add...       |   |
| Outgoing Interface  | lan                   | + |
| Destination Address   | FortiRecorder_HTTPS   | + |
|   | FortiRecorder_RTSP    | + |
|   | FortiRecorder_Central | + |
| Schedule  | always                |   |
| Service   | ALL                   | + |
| Action  | ACCEPT                |   |
| <b>Firewall / Network Options</b>   |                       |   |
| <input checked="" type="checkbox"/> ON NAT  |                       |   |
| <input checked="" type="radio"/> Use Outgoing Interface Address <input type="checkbox"/> Fixed Port |                       |   |
| <input type="radio"/> Use Dynamic IP Pool <input type="text" value="Click to add..."/>              |                       |   |

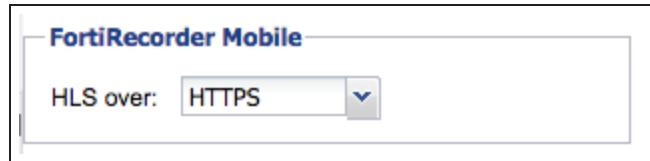


## 6. Configuring FortiRecorder Mobile for iOS

On your FortiRecorder, go to **System > Configuration > Options**.

Set **FortiRecorder Mobile** to use **HLS over HTTPS**.

You can also connect using HLS over HTTP, as long as you add another virtual IP to allow TCP port 80.



### FortiRecorder Mobile for iOS

**Download** the FortiRecorder Mobile app onto your iOS device.

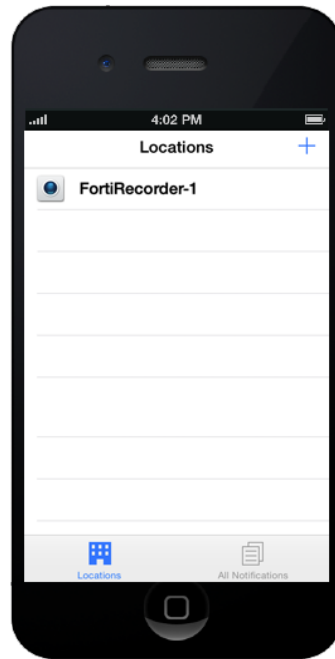
If you will connect using HTTPS, the iOS device must be able to verify the FortiRecorder certificate. To do this, you can either sign the FortiRecorder local certificate with one of the world's largest certificate authorities, whose CA certificate are trusted by the iOS device, or install the CA certificate on the iOS device, if the CA certificate is not trusted by the iOS device. For information about this, see the technical note [Provisioning CA Certificate to iOS Devices for FortiRecorder Mobile](#).

Open FortiRecorder Mobile. Use the **+** to add a new location.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The FortiRecorder is shown in the list of **Locations**.

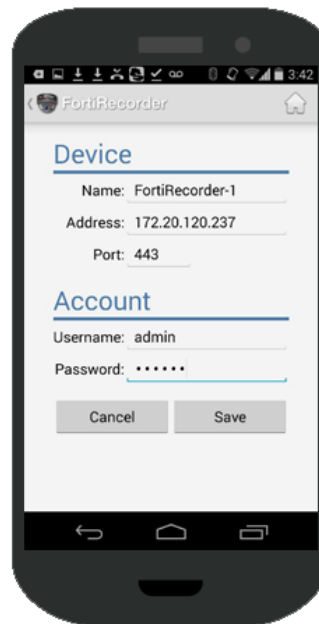


## FortiRecorder Mobile for Android

**Download** the FortiRecorder Mobile app onto your Android device.

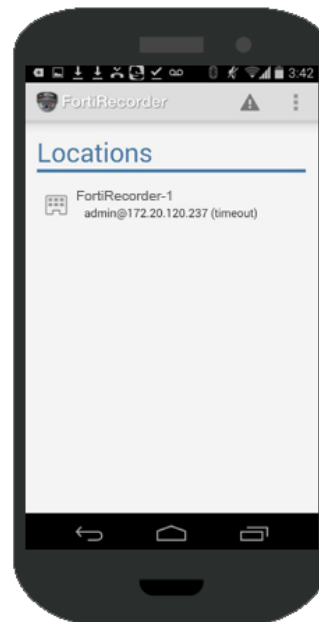
Open FortiRecorder Mobile. Select **Add Location**.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The screenshot shows the FortiRecorder Mobile app interface. At the top, the status bar displays various icons and the time 3:42. The app header shows the FortiRecorder logo and a home icon. The main screen is titled 'Device' and contains two sections: 'Device' and 'Account'. The 'Device' section has three input fields: 'Name' with the value 'FortiRecorder-1', 'Address' with the value '172.20.120.237', and 'Port' with the value '443'. The 'Account' section has two input fields: 'Username' with the value 'admin' and 'Password' with masked characters '\*\*\*\*\*'. At the bottom of the form are two buttons: 'Cancel' and 'Save'. The Android navigation bar is visible at the very bottom.

The FortiRecorder is shown in the list of **Locations**.



The screenshot shows the FortiRecorder Mobile app interface with the 'Locations' screen. The status bar at the top shows the time 3:42. The app header includes the FortiRecorder logo, a warning icon, and a menu icon. The main screen is titled 'Locations' and displays a single entry for 'FortiRecorder-1' with the details 'admin@172.20.120.237 (timeout)'. The Android navigation bar is at the bottom.

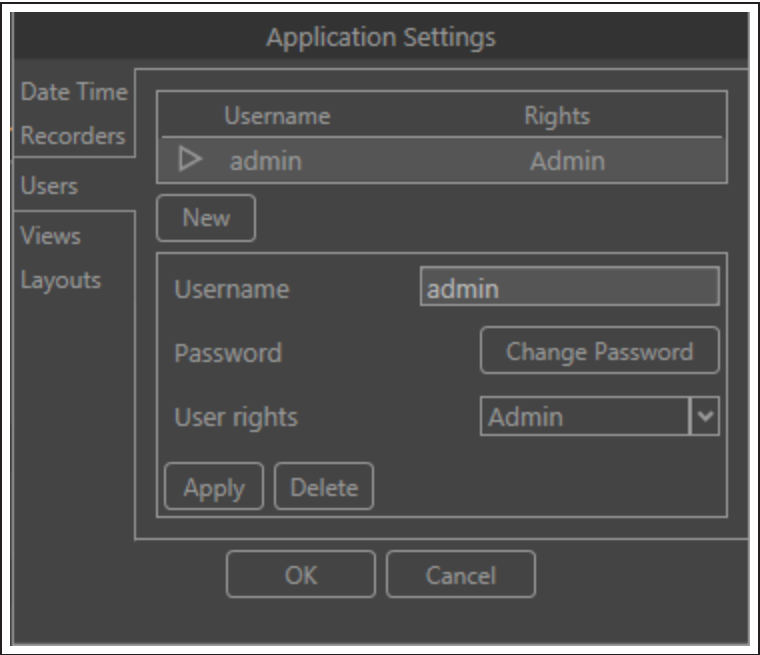
# 7. Configuring FortiRecorder Central

FortiRecorder Central is a Windows-based video management system that is used to connect and view information from several FortiRecorder units at the same time. It can be downloaded at the [Fortinet Support website](#).

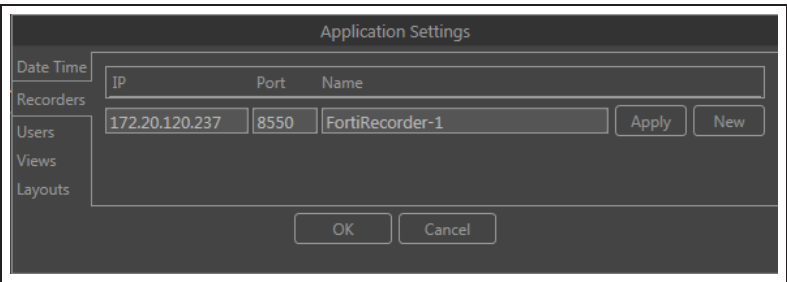
The recipe was written using FortiRecorder Central 1.0.0.

From FortiRecorder Central, use the **Settings** cogwheel in the top right corner to go to **Settings > Users**. Make sure the admin account settings are identical to those on the FortiRecorder because FortiRecorder Central has to be able to log into FortiRecorder using these credentials.

*All FortiRecorders must use the same admin credentials in order to be used by FortiRecorder Central.*



Go to **Settings > Recorders**. Set the IP to the FortiGate's secondary IP (in this example, 172.20.120.237).



The FortiRecorder will appear in the list of devices, with its connected cameras listed underneath.

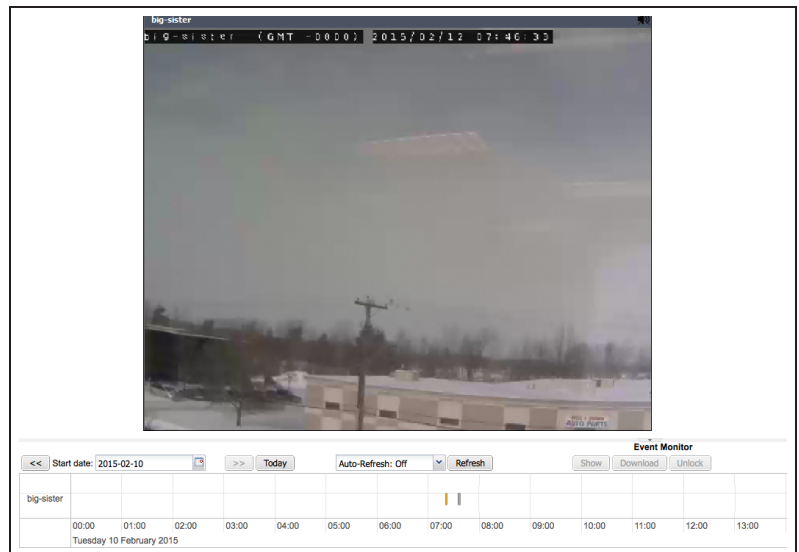


## 8. Results

From the Internet you can browse to the secondary IP address, using HTTPS (in the example, <https://172.20.120.237>). The FortiRecorder GUI login screen appears.

Go to **Monitor > Video Monitor** to see the live video feed from the FortiCamera.

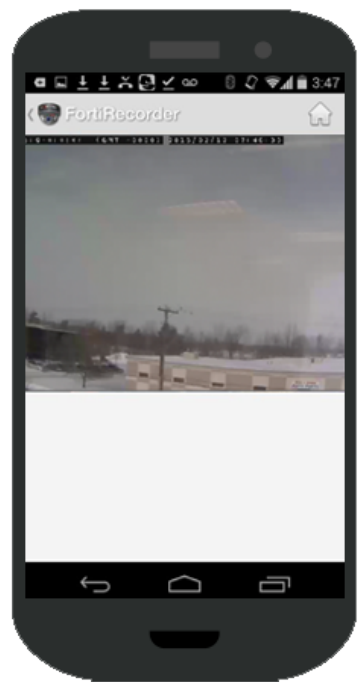
*Quicktime 6.0 or higher is required to view the **Video Monitor**.*



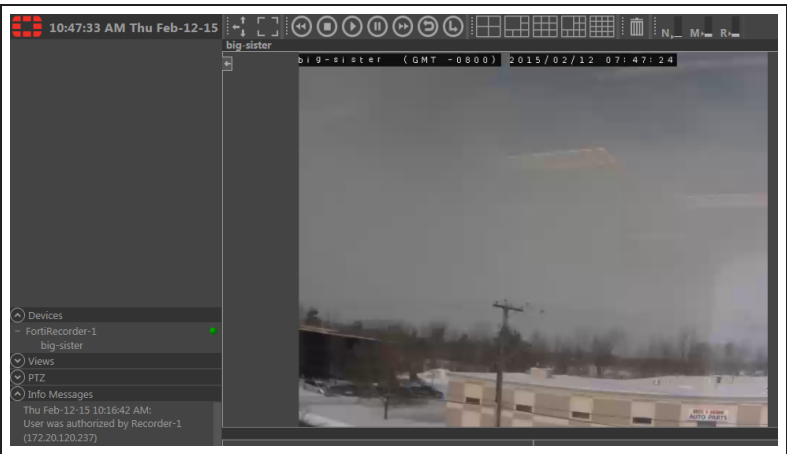
In FortiRecorder Mobile for iOS, go to the **Locations** list and select the FortiRecorder. A list of the available cameras will be shown. Click on the camera you wish to view.



In FortiRecorder Mobile for Android, go to the **Locations** list and select the FortiRecorder, then select **Cameras**. A list of the available cameras will be shown. Click on the camera you wish to view.



In FortiRecorder Central, click on the listing for the FortiCamera and drag it onto a square in the grid. The live video feed will be shown.



# Managing a FortiSwitch with a FortiGate

Manage up to 16 FortiSwitches from the FortiGate web-based manager or CLI. You can create and assign VLANs and configure port information. The connection between the FortiSwitch and the FortiGate is called a FortiLink.

## Prerequisites

- Connect a cable from the highest FortiSwitch port to an unused port on the FortiGate. For example, use port 24 on the FS-224D-POE switch.
- You may need to enable the Switch Controller using the FortiGate web-based manager.
- Go to System > Config > Features.
- Turn on the WiFi & Switch Controller feature.
- Select Apply.
- This recipe is applicable to FortiSwitchOS 3.3.0 and above.

## Procedure

From the FortiGate web-based manager:

1. Go to **System > Network > Interfaces** and edit an internal port.
2. Set **Addressing mode** to **Dedicate to Extension Device**.
3. Select **OK**. The FortiSwitch should now be visible
4. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiSwitch**.  
Right-click on the switch and select **Authorize**.  
-> After a delay (while FortiGate processes the request), an icon with a checkmark appears in the Status column. For smaller FortiSwitch models, such as FS-108D-POE, the delay may be up to 3 minutes.

## Notes

1. In some FortiSwitch models (such as FS-124D), the highest port is an optical interface, which requires an SFP module.
2. In FortiOS 5.4, additional FortiLink features include:
  - a. POE configuration from the FortiGate
  - b. Link Aggregation Group (LAG) support for Fortilink
  - c. Auto-detect the switch FortiLink port. Removes the restriction that only the highest port on the switch can be used for FortiLink
3. Refer to the document below to see the FortiSwitch and FortiGate releases that support FortiLink, and the supported FortiSwitch and FortiGate models in each release.

For additional information, see [Managing FortiSwitch with a FortiGate \(FortiOS 5.2\)](#), which is also available in the [FortiOS 5.2 Handbook](#).



# Authentication

This section contains information about authenticating users and devices.

Authentication, the act of confirming the identity of a person or device, is a key part of network security. When authentication is used, the identities of users or host computers must be established to ensure that only authorized parties can access the network.

## User accounts and device definitions

- [User and device authentication](#)
- [Excluding users from security scanning](#)
- [MAC access control](#)
- [BYOD scheduling](#)
- [BYOD for a user with multiple wireless devices](#)

## Single Sign-On (SSO)

- [FSSO in Polling mode](#)

## Authentication with other technologies

- [Two-factor authentication with FortiToken Mobile](#)

## WiFi local authentication

- [Guest WiFi accounts](#)
- [Captive portal WiFi access control](#)
- [WP2A WiFi access control](#)

## WiFi remote authentication

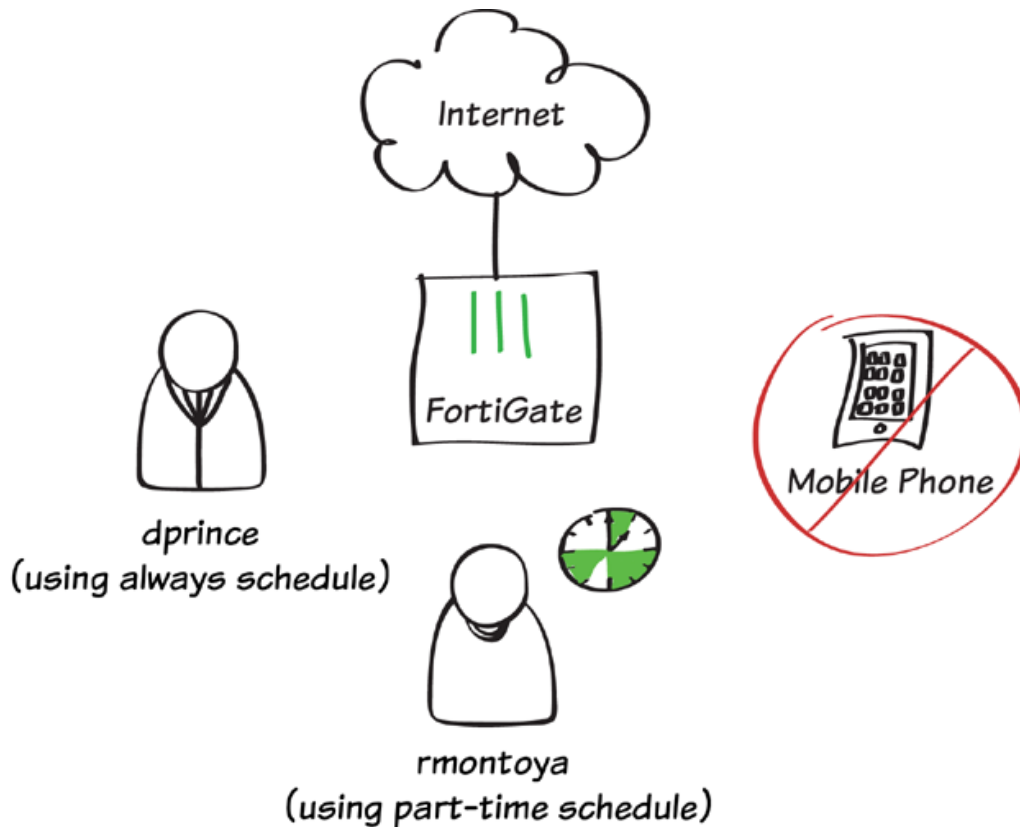
- [WiFi RADIUS authentication with FortiAuthenticator](#)
- [Using an external captive portal for WiFi security](#)
- [Assigning WiFi users to VLANs dynamically](#)
- [WiFi with Wireless Single Sign-on](#)
- [RSSO WiFi access control](#)

- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)

## Authentication for VPNs

- SSL VPN with RADIUS authentication
- RADIUS authentication for SSL VPN with FortiAuthenticator
- LDAP authentication for SSL VPN with FortiAuthenticator
- SSL VPN remote browsing with LDAP authentication
- SSL VPN with certificate authentication
- SMS two-factor authentication for SSL VPN
- IPsec VPN with two-factor authentication

# User and device authentication



In this example, user authentication and device authentication provide different access for staff members based on whether they are full-time or part-time employees, while denying all traffic from mobile phones.

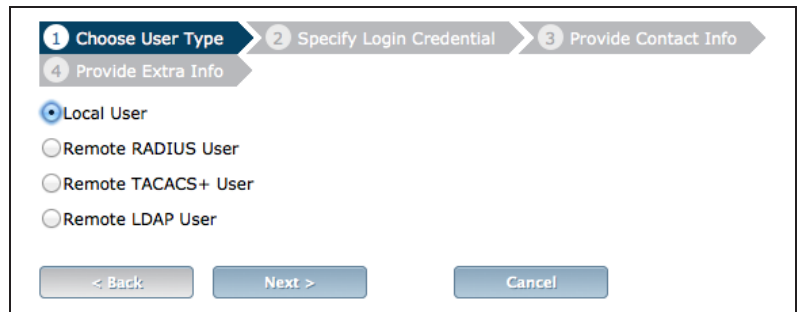
In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, see [Setting up a WiFi bridge with a FortiAP](#).

A video of this recipe can be found [here](#).

## 1. Defining two users and two user groups

Go to **User & Device > User > User Definitions**.

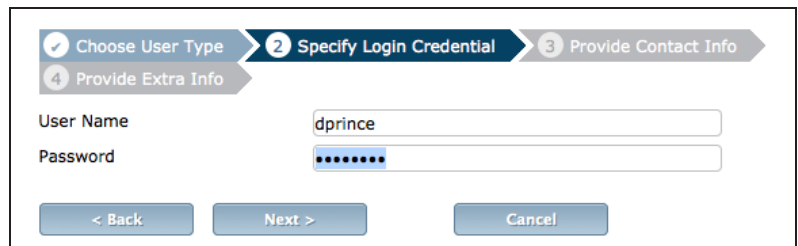
Create two new users (in the example, *dprince* and *montoya*).



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

☒ Local User  
☐ Remote RADIUS User  
☐ Remote TACACS+ User  
☐ Remote LDAP User

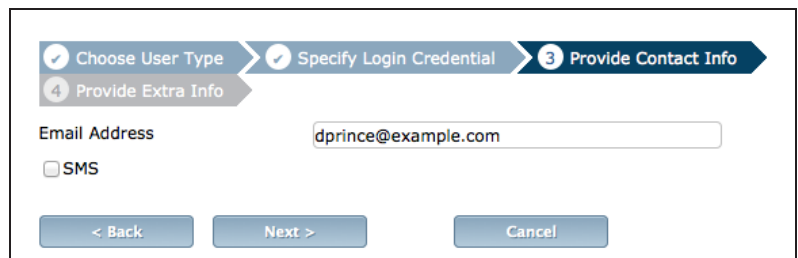
< Back Next > Cancel



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

User Name dprince  
Password .....

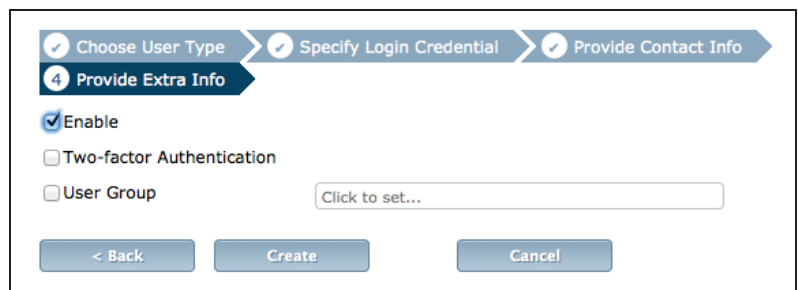
< Back Next > Cancel



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Email Address dprince@example.com  
☐ SMS

< Back Next > Cancel



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

☒ Enable  
☐ Two-factor Authentication  
☐ User Group Click to set...

< Back Create Cancel

Both user definitions now appear in the user list.

| User Name | Type  | Two-factor Authentication | Ref. |
|-----------|-------|---------------------------|------|
| dprince   | LOCAL |                           | 0    |
| guest     | LOCAL |                           | 1    |
| rmontoya  | LOCAL |                           | 0    |

Go to **User & Device > User > User Groups**.

Create the user group *full-time* and add user *dprince*.

Name

full-time

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

dprince

Create a second user group, *part-time*, and add user *rmontoya*.

Name

part-time

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

rmontoya

## 2. Creating a schedule for part-time staff

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

Set an appropriate schedule. In order to get results later, do not select the current day of the week.

Type

☒ Recurring ☐ One-time

Name

part-time

Days

☐ Sunday ☒ Monday ☐ Tuesday ☒ Wednesday ☐ Thursday ☒ Friday ☐ Saturday

Start Time

Hour

0

:

Minute

0

:

Stop Time

Hour

0

:

Minute

0

:

## 3. Defining a device group for mobile phones

Go to **User & Device > Device > Device Groups** and create a new group.

Add the various types of mobile phones as **Members**.

Name

mobile-phones

Members

Android Phone

BlackBerry Phone

Windows Phone

iPhone

Comments

Write a comment...

0/255

## 4. Creating a policy for full-time staff

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the full-time group, **Outgoing Interface** to your Internet-facing interface, and ensure that **Schedule** is set to **always**.

Turn on **NAT**.

Incoming Interface: lan  
Source Address: all  
Source User(s): full-time  
Source Device Type: Click to add...  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: always  
Service: ALL  
Action: ACCEPT

**Firewall / Network Options**  
☒ NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

**Logging Options**  
☒ Log Allowed Traffic  
☐ Security Events  
☒ All Sessions  
☐ Capture Packets

## 5. Creating a policy for part-time staff that enforces the schedule

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the part-time group, **Outgoing Interface** to your Internet-facing interface, and set **Schedule** to use the part-time schedule.

Turn on **NAT**.

Incoming Interface: lan  
Source Address: all  
Source User(s): part-time  
Source Device Type: Click to add...  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: part-time  
Service: ALL  
Action: ACCEPT

**Firewall / Network Options**  
☒ NAT  
☒ Use Destination Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

**Logging Options**

ON

Log Allowed Traffic

☐ Security Events

☒ All Sessions

☐ Capture Packets

View the policy list. Click on the title row and select **ID** from the dropdown menu, then select **Apply**. Take note of the ID number that has been given to the part-time policy.

| Seq.# | From | To   | Schedule  | Source           | Destination | ID |
|-------|------|------|-----------|------------------|-------------|----|
| 1     | lan  | wan1 | always    | all<br>full-time | all         | 1  |
| 2     | lan  | wan1 | part-time | all<br>part-time | all         | 2  |
| 3     | any  | any  | always    | all              | all         |    |

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**, using the ID number of the part-time policy.

This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

```
config firewall policy
edit 2
set schedule-timeout enable
end
end
```

## 6. Creating a policy that denies mobile traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source Device** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and set **Action** to **DENY**.

*Using a device group will automatically enable device identification on the local network interface.*

Leave **Log Violation Traffic** turned on.

In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

Incoming Interface

lan

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

mobile-phones

×

+

Outgoing Interface

wan1

+

Destination Address

all

+

Schedule

always

Service

ALL

+

Action

DENY

Logging Options

ON

Log Violation Traffic

| Seq.# | From | To   | Devices        | Groups    | Action |
|-------|------|------|----------------|-----------|--------|
| 3     | lan  | wan1 | Mobile Devices |           | DENY   |
| 1     | lan  | wan1 |                | full-time | ACCEPT |
| 2     | lan  | wan1 |                | part-time | ACCEPT |
| 4     | any  | any  |                |           | DENY   |



## 7. Results

Browse the Internet using a computer.  
You will be prompted to enter authentication credentials.



Log in using the *dprince* account. You will be able to access the Internet at any time.



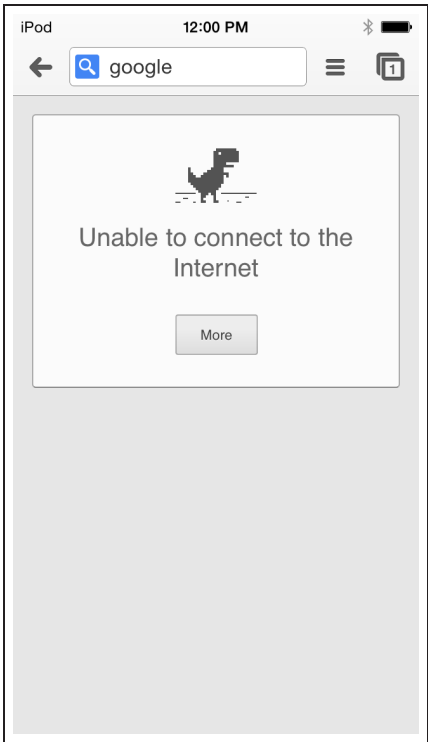
The image shows a Fortinet authentication dialog box. At the top is the Fortinet logo. Below it, the text "Authentication Required" is displayed. A message says "Please enter your username and password to continue." There are two input fields: "Username:" and "Password:", each followed by a small asterisk icon. A "Continue" button is located at the bottom right of the dialog.

Go to **User & Device > Monitor > Firewall**. Highlight **dprince** and select **De-authenticate**.

Attempt to browse the Internet again.  
This time, log in using the *montoya* account. After authentication occurs, you will not be able to access the Internet.

|  Refresh |  De-authenticate |
|---|---|
| User Name   | User Group  |
| dprince   | full-time   |

Attempts to connect to the Internet using any mobile phone will also be denied.



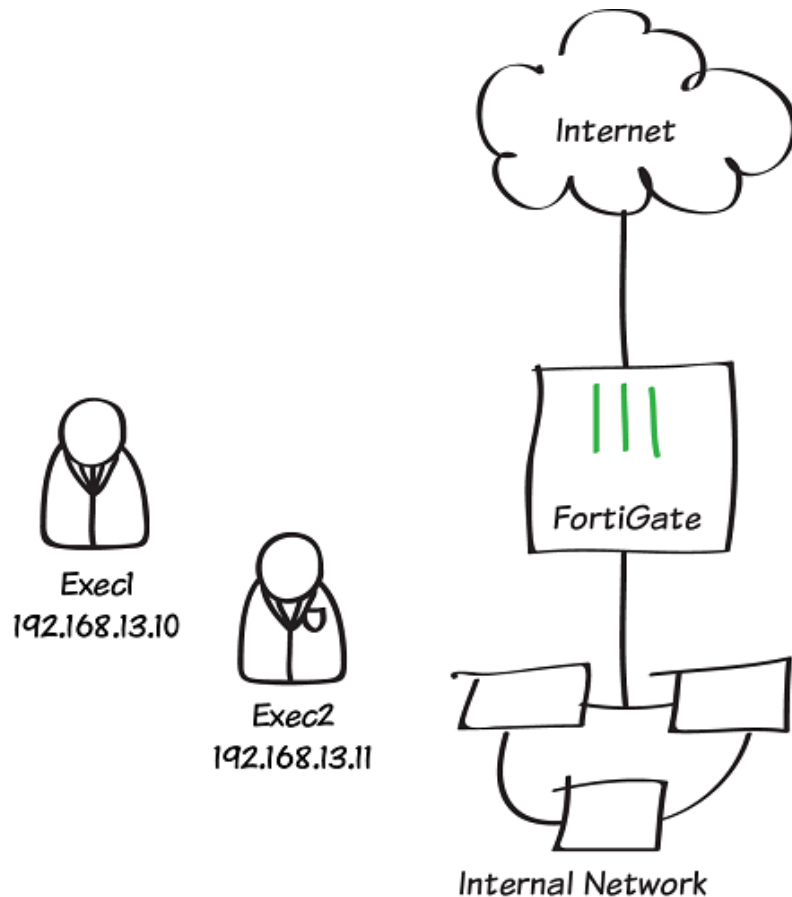
You can view more information about the blocked and allowed sessions by going to **System > FortiView > All Sessions**.

*Sessions that were blocked when you attempted to sign in using the montoya account will not have a user account shown in the **User** column.*

| Date/Time | User    | Device   | Destination                                     | Action |
|-----------|---------|----------|---|--------|
| 09:10:21  |         | iPhone   | 208.91.112.53                                   | deny   |
| 09:10:21  |         | Mac Mini | 157.55.56.159                                   | deny   |
| 09:10:21  |         | Mac Mini | 111.221.74.30                                   | deny   |
| 09:10:21  |         | Mac Mini | 111.221.77.159                                  | deny   |
| 09:10:21  |         | iPhone   | 208.91.112.52                                   | deny   |
| 09:10:20  |         | iPhone   | 208.91.112.53                                   | deny   |
| 09:10:20  |         | iPhone   | 208.91.112.53                                   | deny   |
| 09:10:19  |         | Mac Mini | 157.55.56.159                                   | deny   |
| 09:10:19  |         | Mac Mini | 157.56.52.30                                    | deny   |
| 09:10:17  |         | iPhone   | 208.91.112.52                                   | deny   |
| 09:10:17  | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com)              | accept |
| 09:10:16  | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com)              | accept |
| 09:10:16  | dprince | Mac Mini | 54.231.0.33 (s3-1-w.amazonaws.com)              | accept |
| 09:10:15  | dprince | Mac Mini | 64.94.107.34 (map-pb.quantserve.com.akadns.net) | accept |
| 09:10:15  | dprince | Mac Mini | 174.36.240.82 (api.mixpanel.com)                | accept |

For further reading, check out **Users and user groups** in the **FortiOS 5.2 Handbook**.

# Excluding users from security scanning



In this example, two company executives are excluded from the security scanning that a FortiGate applies to all other staff Internet traffic.

The executives in this example connect to the Internet using PCs with static IP addresses, so these addresses can be used to identify their traffic. If identifying users with a static IP address will not work for your network you can set up authentication or device identification (BYOD).

# 1. Applying security profiles to the staff policy

Go to **Policy & Objects > Policy > IPv4** and edit the general policy that allows staff to access the Internet.

Under **Security Profiles**, enable **Web Filter** and **Application Control**. Set them to use the default profiles. Also set **SSL/SSH Insection** to the **deep-inspection** profile.

To be able to see results enable logging all sessions.

|   |                                     |   |
|---|-------------------------------------|---|
| Incoming Interface  | internal                            | + |
| Source Address  | Internal-net                        | + |
| Source User(s)  | Click to add...                     |   |
| Source Device Type  | Click to add...                     |   |
| Outgoing Interface  | wan1                                | + |
| Destination Address   | all                                 | + |
| Schedule  | always                              |   |
| Service   | ALL                                 | + |
| Action  | ACCEPT                              |   |
| <b>Firewall / Network Options</b>                               |                                     |   |
| <input checked="" type="checkbox"/> NAT                         |                                     |   |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port |   |
| <input type="radio"/> Use Dynamic IP Pool                       | Click to add...                     |   |
| <b>Security Profiles</b>  |                                     |   |
| <input type="checkbox"/> AntiVirus                              | default                             | + |
| <input checked="" type="checkbox"/> Web Filter                  | default                             | + |
| <input checked="" type="checkbox"/> Application Control         | default                             | + |
| Proxy Options   | default                             | + |
| <input checked="" type="checkbox"/> SSL/SSH Inspection          | certificate-inspection              | + |
| <b>Logging Options</b>  |                                     |   |
| <input checked="" type="checkbox"/> Log Allowed Traffic         |                                     |   |
| <input type="checkbox"/> Security Events                        |                                     |   |
| <input checked="" type="radio"/> All Sessions                   |                                     |   |

# 2. Creating firewall addresses for the executives

Go to **Policy & Objects > Objects > Addresses**. Create an address for each executive. Use /32 as the Netmask to ensure that the firewall address applies only to the specified IP.

|                      |                                     |
|----------------------|-------------------------------------|
| Name                 | Exec1                               |
| Type                 | IP/Netmask                          |
| Subnet / IP Range    | 192.168.13.10                       |
| Interface            | internal                            |
| Show in Address List | <input checked="" type="checkbox"/> |
| Comments             |                                     |

|                      |                                     |
|----------------------|-------------------------------------|
| Name                 | Exec2                               |
| Type                 | IP/Netmask                          |
| Subnet / IP Range    | 192.168.13.11                       |
| Interface            | internal                            |
| Show in Address List | <input checked="" type="checkbox"/> |
| Comments             | <input type="text"/> 0/255          |

Select **Create New > Address Group** and create an address group for the executive addresses.

|                      |   |
|----------------------|---|
| Group Name           | Executives                              |
| Show in Address List | <input checked="" type="checkbox"/>     |
| Members              | <div>Exec1 X +</div> <div>Exec2 X</div> |

### 3. Creating a security policy for the executives

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing the executives to access the Internet. Set **Source Address to Executives**. Enable logging and select Log all Sessions to be able to view results.

Leave all Security Profiles disabled.

|   |                                     |   |
|---|-------------------------------------|---|
| Incoming Interface  | internal                            | + |
| Source Address  | Executives                          | + |
| Source User(s)  | Click to add...                     |   |
| Source Device Type  | Click to add...                     |   |
| Outgoing Interface  | wan1                                | + |
| Destination Address   | all                                 | + |
| Schedule  | always                              |   |
| Service   | ALL                                 | + |
| Action  | ACCEPT                              |   |
| <b>Firewall / Network Options</b>                               |                                     |   |
| <input checked="" type="checkbox"/> NAT                         |                                     |   |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port |   |
| <input type="radio"/> Use Dynamic IP Pool                       | Click to add...                     |   |
| <b>Security Profiles</b>  |                                     |   |
| <input type="checkbox"/> AntiVirus                              | default                             |   |
| <input type="checkbox"/> Web Filter                             | default                             |   |
| <input type="checkbox"/> Application Control                    | default                             |   |
| <input type="checkbox"/> SSL/SSH Inspection                     | certificate-inspection              |   |
| <b>Logging Options</b>  |                                     |   |
| <input checked="" type="checkbox"/> Log Allowed Traffic         |                                     |   |
| <input type="radio"/> Security Events                           |                                     |   |
| <input checked="" type="radio"/> All Sessions                   |                                     |   |

In the policy list, the policy for executives (in this example ID=3) must be above the policy for staff (in this example ID=2).

You can re-order policies by hovering your mouse cursor over the borders of the left-most cell of a policy until the cursor changes into crossed arrows and then clicking and dragging that policy up or down into the required order.

Note that in this screen shot the policy ID (ID) is shown for each policy and the sequence number (Seq.#) is hidden.

| ID                  | Source       | Destination | Schedule | Service | Action | NAT    | AV | Web Filter | Application Control |
|---------------------|--------------|-------------|----------|---------|--------|--------|----|------------|---------------------|
| internal - wan1 (2) |              |             |          |         |        |        |    |            |                     |
| 3                   | Executives   | all         | always   | ALL     | ACCEPT | Enable |    |            |                     |
| 2                   | Internal-net | all         | always   | ALL     | ACCEPT | Enable |    | default    | default             |

## 4. Results

Connect to the Internet from two computers on the internal network: one from an executive address and one from a staff address.

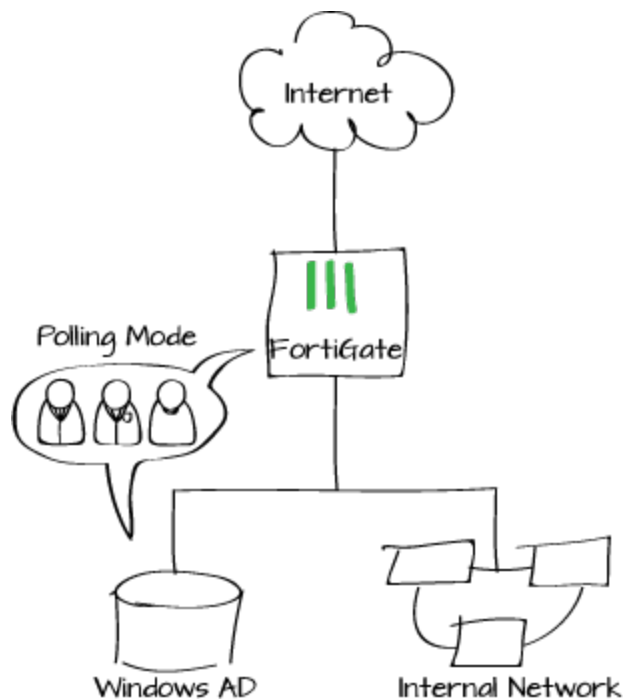
Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click the column headings and make sure that the **Policy** ID column is visible.

In this example output, connections from 192.168.13.10 (an executive address) use policy ID 3 and connections from 192.168.13.144 (a staff address) use policy ID 2.

| #  | Policy ID | Date/Time | Source         | Sent / Received    |
|----|-----------|-----------|----------------|--------------------|
| 1  | 3         | 07:46:28  | 192.168.13.10  | 1.11 KB / 10.99 KB |
| 2  | 3         | 07:46:28  | 192.168.13.10  | 1.10 KB / 9.13 KB  |
| 3  | 3         | 07:46:28  | 192.168.13.10  | 1.07 KB / 9.51 KB  |
| 4  | 3         | 07:46:28  | 192.168.13.10  | 1.16 KB / 12.48 KB |
| 5  | 3         | 07:46:28  | 192.168.13.10  | 1.12 KB / 11.14 KB |
| 6  | 2         | 07:45:48  | 192.168.13.144 | 8.41 KB / 10.79 KB |
| 7  | 2         | 07:45:24  | 192.168.13.144 | 653 B / 4.99 KB    |
| 8  | 2         | 07:44:57  | 192.168.13.144 | 48 B / 0 B         |
| 9  | 2         | 07:44:47  | 192.168.13.144 | 2.51 KB / 1.28 KB  |
| 10 | 2         | 07:44:47  | 192.168.13.144 | 3.49 KB / 5.99 KB  |

For further reading, check out [Security Profiles](#) in the [FortiOS 5.2 Handbook](#).

# FSSO in Polling mode



In this example, you will configure Fortinet Single Sign-On (FSSO) directly in the security policy using the new FSSO wizard introduced in FortiOS 5.2.2.

*This recipe requires that your FortiGate's DNS point to a DNS server that can resolve the IP addresses or fully qualified domain names of the users' PCs.*

This example uses Active Directory polling to establish FSSO for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a collector agent to act as an intermediary between the FortiGate and the domain. An LDAP server is also used for authentication.

A video of this recipe is available [here](#).

## 1. Adding the LDAP Server to the FortiGate

In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**.

For the **Server IP/Name** enter the LDAP Server's fully qualified domain name or the IP address.

Set the **Bind Type** to **Regular** and enter a **User DN** and **Password**.

Click **Fetch DN** to retrieve your **Distinguished Name**.

**Edit LDAP Server**

Name: FAC\_LDAP

Server IP/Name: 172.20.120.132

Server Port: 389

Common Name Identifier: cn

Distinguished Name: dc=fortidocs,dc=com

Bind Type: ☐ Simple ☐ Anonymous ☒ Regular

User DN: example\_admin

Password: .....

☐ Secure Connection

Test

OK Cancel

Click **Test** and verify that your connection is successful.



## 2. Configuring the FortiGate unit to poll the Active Directory

Next, go to **User & Device > Authentication > Single Sign-On** and add a new Single Sign-On Server.

For the **Type**, select **Poll Active Directory Server**. Enter the **Server IP/Name**, **User**, and **Password**, then select the **LDAP Server** you added previously. Make sure **Enable Polling** is checked. Add a test user group of your choice.

*You must add at least one user group to create your SSO server.*

**New Single Sign-On Server**

Type: ☒ Poll Active Directory Server ☐ Fortinet Single-Sign-On Agent ☐ RADIUS Single-Sign-On Agent

Server IP/Name: 172.20.120.132

User: example\_admin

Password: .....

LDAP Server: FAC\_LDAP

Enable Polling: ☒

Users/Groups

LDAP Tree Recursive: ON

DC=fortidocs,DC=com

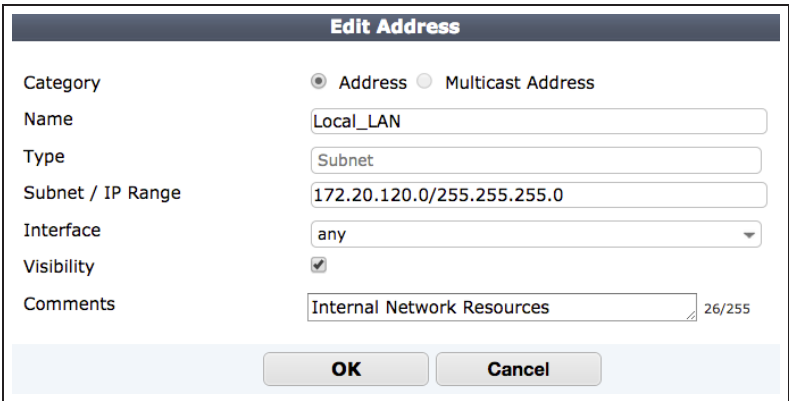
| ID                                      | Name                                    | CN     |
|---|---|--------|
| Account Operators                       | Account Operators                       | CN=Ac  |
| Administrators                          | Administrators                          | CN=Ad  |
| Allowed RODC Password Replication Group | Allowed RODC Password Replication Group | CN=All |
| Backup Operators                        | Backup Operators                        | CN=Ba  |
| Cert Publishers                         | Cert Publishers                         | CN=Ce  |

1 / 2 [ Total: 54 ]



### 3. Adding a firewall address for the Internal network

Go to **Policy & Objects > Objects > Addresses** and create an internal network address to be used by your security policy.



**Edit Address**

Category: ☒ Address ☐ Multicast Address

Name: Local\_LAN

Type: Subnet

Subnet / IP Range: 172.20.120.0/255.255.255.0

Interface: any

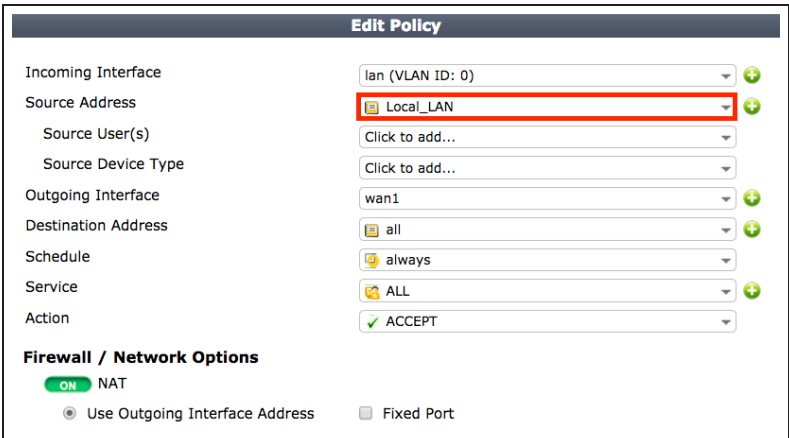
Visibility: ☒

Comments: Internal Network Resources 26/255

OK Cancel

### 4. One-step FSSO configuration in the security policy

Go to **Policy & Objects > Policy > IPv4** and edit a security policy with access to the Internet. Set the **Source Address** to the **Local\_LAN** address created in **Step 3**.



**Edit Policy**

Incoming Interface: lan (VLAN ID: 0)

Source Address: Local\_LAN

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

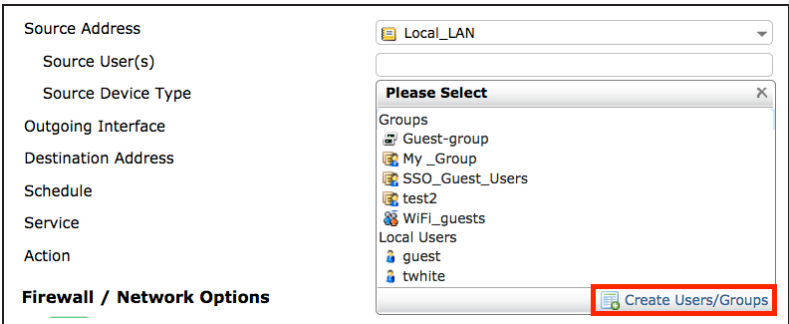
Action: ACCEPT

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

Under **Source User(s)** scroll down past the dropdown menu, and select **Create Users/Groups** wizard.



**Edit Policy**

Source Address: Local\_LAN

Source User(s): Please Select

Source Device Type: Please Select

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

Groups: Guest-group, My\_Group, SSO\_Guest\_Users, test2, WIFI\_guests

Local Users: guest, twhite

Create Users/Groups

For the **User/Group Type**, select **FSSO** and then click **Next**.

1 User/Group Type 2 Remote Groups 3 Local Group

- ☐ Local User
- ☐ Remote RADIUS User
- ☐ Remote TACACS+ User
- ☐ Remote LDAP User
- ☒ FSSO

< Back Next > Cancel

For the **Remote Group**, select the appropriate **FSSO Agent** from the dropdown menu.

Select the **Groups** tab and right-click on the user groups you would like to add.

*To add multiple groups, hold the Shift key and click.*

1 User/Group Type 2 Remote Groups 3 Local Group

FSSO Agent 172.20.120.132

LDAP Server FAC\_LDAP

LDAP Users/Groups

LDAP Tree Recursive ON

dc=fortidocs,dc=com

Users Groups Selected (0)

+ Add Selected

| ID                          | Name                        |         |
|-----------------------------|-----------------------------|---------|
| Session Directory Computers | Session Directory Computers | CN=Sess |
| Standard_User_Group         | Standard_User_Group         | CN=Star |
| TechDoc                     | TechDoc                     | CN=Tech |
| Terminal Server Computers   | Terminal Server Computers   | CN=Terr |

< Back Next > Cancel

Go to the **Selected** tab. In this example, **Standard\_User\_Group** and **Admin\_User\_Group** are shown.

Click **Next**.

1 User/Group Type 2 Remote Groups 3 Local Group

FSSO Agent 172.20.120.132

LDAP Server FAC\_LDAP

LDAP Users/Groups

LDAP Tree Recursive ON

dc=fortidocs,dc=com

Users Groups Selected (2)

X Remove Selected

| ID                       | Name                     | First Name | Last |
|--------------------------|--------------------------|------------|------|
| Standard_User_Group      | Standard_User_Group      |            |      |
| Administrator_User_Group | Administrator_User_Group |            |      |

< Back Next > Cancel

Select **Create New** and name your new FSSO user group.

Click **Create**.

User/Group TypeRemote GroupsLocal Group

Add to FSSO Group

☐ Choose Existing

☒ Create New

Click to set...

My\_Windows\_AD\_Group

< Back

Create

Cancel

The groups selected have been added to the new FSSO group, **My\_Windows\_AD\_Group**.

To see these groups go to **User & Device > User > User Groups**.

Create NewEditDelete

Search

| Group Name                      | Group Type                     | Members   | Ref. |
|---------------------------------|--------------------------------|---|------|
| Guest-group (1 Members)         | Firewall                       | guest   | 0    |
| My_Windows_AD_Group (2 Members) | Fortinet Single Sign-On (FSSO) | CN=Administrator_User_Gro...CN=Standard_User_Group,C... | 1    |
| SSO_Guest_Users (0 Members)     | Fortinet Single Sign-On (FSSO) |   | 0    |
| WiFi_guests (0 Members)         | Guest                          |   | 0    |

Ensure you enable logging and select **All Sessions**.

Logging Options

ON

Log Allowed Traffic

☐ Security Events

☒ All Sessions

In the **Global View** your completed policy should look similar to the screenshot shown on the right.

If necessary, select the policy by clicking on the far left column, and move it as close as possible to the top of the list.

All other policies must deny Internet access in order for the user to be forced to authenticate.

Create NewEditDelete

Section ViewGlobal ViewSearch

| Seq.# | From | To   | Source                           | Action | Destination | Schedule | NAT    | Serv |
|-------|------|------|----------------------------------|--------|-------------|----------|--------|------|
| 1     | lan  | wan1 | Local_LAN<br>My_Windows_AD_Group | ACCEPT | all         | always   | Enable | ALL  |
| 2     | any  | any  | all                              | DENY   | all         | always   |        | ALL  |

## 5. Results





Go to **Log & Report > Traffic Log > Forward Traffic**.

When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

RefreshDownload Raw Log

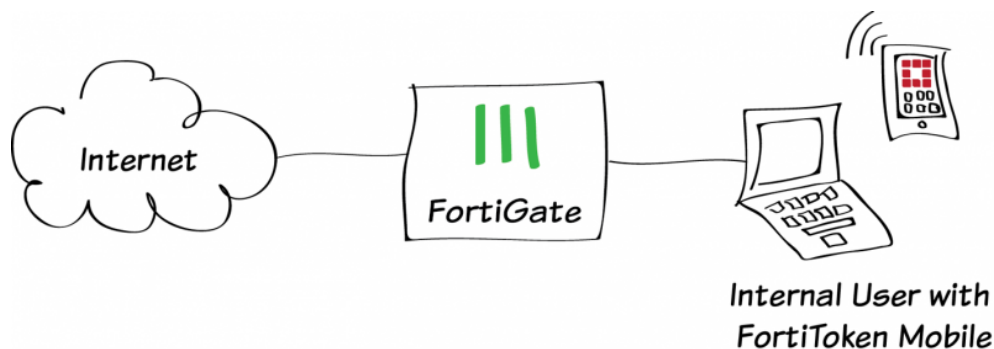
| # | Date/Time | Source                 | Destination    | Sent / Received    | Application Name | Device    |
|---|-----------|------------------------|----------------|--------------------|------------------|-----------|
| 1 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 3.04 KB / 33.74 KB | HTTP             | BDAVIS-NB |
| 2 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 1.00 KB / 2.34 KB  | HTTP             | BDAVIS-NB |
| 3 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 1.53 KB / 19.79 KB | HTTP             | BDAVIS-NB |
| 4 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 1.06 KB / 6.99 KB  | HTTP             | BDAVIS-NB |
| 5 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 585 B / 950 B      | HTTP             | BDAVIS-NB |
| 6 | 16:21:26  | twhite (172.20.120.68) | 192.168.27.100 | 595 B / 735 B      | HTTP             | BDAVIS-NB |

Select an entry for more information.

|                     |   |                 |   |
|---------------------|---|-----------------|---|
| #                   | 1   | Action          | deny  |
| Date/Time           | 17:52:19  | Destination     | 192.168.27.100  |
| Destination Country | Reserved  | Device          |  BDAVIS-NB               |
| Device Type         | Windows PC  | Dst Interface   | wan1  |
| Duration            | 5526  | Group           | test2   |
| Level               |  | Log ID          | 13  |
| Master Src MAC      | f0:4d:a2:c5:7c:f4   | OS Name         | Windows 7 / Windows   |
| Policy ID           | 0   | Policy UUID     | d5e34b16-80ba-51e4-4f4a-5dc0ab93d7e0  |
| Protocol            | icmp  | Protocol Number | 1   |
| Received            | 328140  | Sent            | 328800  |
| Sent Packets        | 5480  | Sequence Number | 974328  |
| Service             | PING  | Source          |  twwhite (172.20.120.68) |
| Source Country      | Reserved  | Src Interface   | lan   |
| Src NAT IP          | 192.168.27.1  | Src NAT Port    | 0   |
| Src Name            | BDAVIS-NB   | Sub Type        | forward   |
| Threat              | 131072  | Threat Level    | high  |
| Threat Score        | 30  | Timestamp       | 12/15/2014, 5:52:19 PM  |
| Tran Display        | snat  | User            |  twwhite                 |
| Virtual Domain      | root  |                 |   |

For further reading, check out [Single Sign-On to Windows AD in the FortiOS 5.2 Handbook](#).

# Two-factor authentication with FortiToken Mobile



In this recipe, two-factor authentication is added to a user account to provide extra security to the authentication process.

Two-factor authentication requires a user to provide further means of authentication in addition to their credentials. In this recipe, FortiToken Mobile app for Android will be used to generate a token, also known as a one-time password (OTP), to use in the authentication process.

A video of this recipe is available [here](#).

## 1. Activating your FortiTokens

Ensure that your FortiGate is connected to the Internet. Go to **User & Device > FortiTokens**. Your FortiGate may have two FortiToken Mobile entries listed by default. If so, you may use these tokens and go to step 2.











To add new FortiTokens, select **Create New**. Set **Type** to **Mobile Token** and enter your **Activation Code**.

*An error stating that the serial number is invalid will appear if you mistyped the code or if it duplicates one you have already entered.*

After FortiGuard validates the code, your FortiTokens will appear on the list, with **Status** set to **Available**

*If the FortiToken has already been registered to another FortiGate, the **Status** will be **Error**.*

|                 |  |
|-----------------|--|
| Type            | <input type="radio"/> Hard Token <input checked="" type="radio"/> Mobile Token |
| Activation Code | <input type="text" value="0000-0000-0000-0000-0000"/>                          |

| Type  | Serial Number       | Status  |
|---|---------------------|---|
|  | FTKMOB4A [REDACTED] |  Available |
|  | FTKMOB4A [REDACTED] |  Available |
|  | FTKMOB4A [REDACTED] |  Available |
|  | FTKMOB4A [REDACTED] |  Available |
|  | FTKMOB4A [REDACTED] |  Available |

## 2. Creating a user account with two-factor authentication

Go to **User & Device > User > User Definition** and create a new local user.

|   |                            |                        |                      |
|---|----------------------------|------------------------|----------------------|
| 1 Choose User Type                          | 2 Specify Login Credential | 3 Provide Contact Info | 4 Provide Extra Info |
| <input checked="" type="radio"/> Local User |                            |                        |                      |
| <input type="radio"/> Remote RADIUS User    |                            |                        |                      |
| <input type="radio"/> Remote TACACS+ User   |                            |                        |                      |
| <input type="radio"/> Remote LDAP User      |                            |                        |                      |
| < Back                                      |                            | Next >                 | Cancel               |

|   |                            |                        |                      |
|---|----------------------------|------------------------|----------------------|
| 1 Choose User Type                              | 2 Specify Login Credential | 3 Provide Contact Info | 4 Provide Extra Info |
| User Name <input type="text" value="coswald"/>  |                            |                        |                      |
| Password <input type="password" value="*****"/> |                            |                        |                      |
| < Back  |                            | Next >                 | Cancel               |

In order to use the FortiToken Mobile, you must enter a mobile number in the third step, **Provide Contact Info**. Select the appropriate **Country/Region** and enter the **Phone Number** without dashes or spaces. Do *not* add an email address.

Choose User TypeSpecify Login Credential3 Provide Contact Info4 Provide Extra Info

Email Address

☒ SMS

Country/Region

United States/Canada

Phone Number

+1

Service Type

FortiGuard Messaging Service

< Back

Next >

Cancel

In the fourth step of the User Creation Wizard, **Provide Extra Info**, enable **Two-Factor Authentication** and select an available token.

Choose User TypeSpecify Login CredentialProvide Contact Info4 Provide Extra Info

☒ Enable

☒ Two-factor Authentication

Token

FTKMOB4A3CF4DCA3

☐ User Group



Click to set...

< Back




Create

Cancel

The user list shows the FortiToken in the **Two-factor Authentication** column for the new user account.

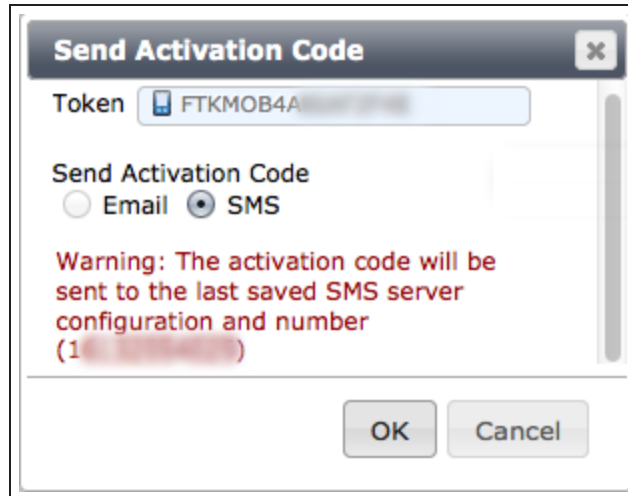
| User Name▲ | Type  | Two-factor Authentication  |
|------------|---|--|
| coswald    |  LOCAL |  FTKMOB4A86AF2F4B |

Go to **User & Device > FortiTokens**. The FortiToken assigned to the user is now listed as **Pending**, until the user activates the FortiToken.

| Type  | Serial Number    | Status  | User  |
|---|------------------|---|---|
|  | FTKMOB4A86AF2F4B |  Pending |  coswald |

### 3. Sending the activation code to the user

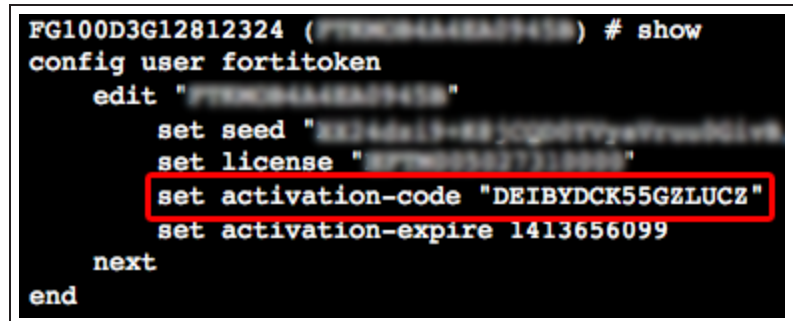
If your FortiGate can send SMS messages, go to **User & Device > User > User Definition** and edit the new user account. Select **Send Activation Code** and send the code by **SMS**.

A screenshot of the 'Send Activation Code' dialog box in FortiGate. The dialog has a title bar with a close button. Below the title, there is a 'Token' field with a mobile phone icon and the text 'FTKMOB4A'. Underneath, there are two radio buttons: 'Email' and 'SMS', with 'SMS' being selected. A red warning message states: 'Warning: The activation code will be sent to the last saved SMS server configuration and number (123456789)'. At the bottom, there are 'OK' and 'Cancel' buttons.

If your FortiGate cannot send SMS messages, go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct serial number:

```
config user fortitoken
edit serial number
show
```

The activation code will be shown in the output. This code must be given to the user.

A screenshot of a FortiGate CLI console session. The prompt is 'FG100D3G12812324 (PTK100D3G12812324) #'. The user enters 'show config user fortitoken'. The output shows the configuration for 'fortitoken', including 'set seed', 'set license', 'set activation-code', and 'set activation-expire'. The 'set activation-code' line, which contains the code 'DEIBYDCK55GZLUCZ', is highlighted with a red rectangle. The session ends with 'next' and 'end' commands.

```
FG100D3G12812324 (PTK100D3G12812324) # show
config user fortitoken
edit "PTK100D3G12812324"
set seed "3324da19-88-jcgn677yefrwe8d1v8"
set license "8PTM03327310000"
set activation-code "DEIBYDCK55GZLUCZ"
set activation-expire 1413656099
next
end
```



## 4. Adding user authentication to your Internet access policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet. Set **Source User(s)** to the new user account.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | port3           |
| Source Address      | all             |
| Source User(s)      | coswald         |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address | all             |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

**Firewall / Network Options**

☒ ON NAT

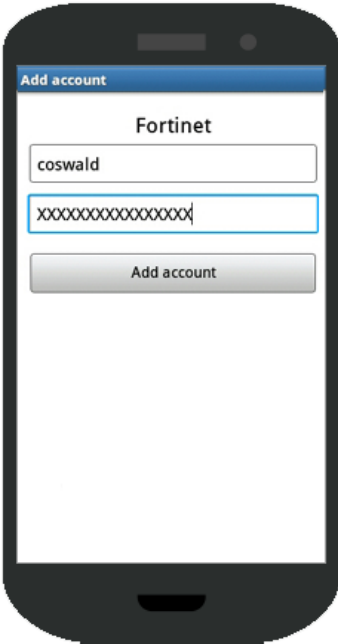
☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

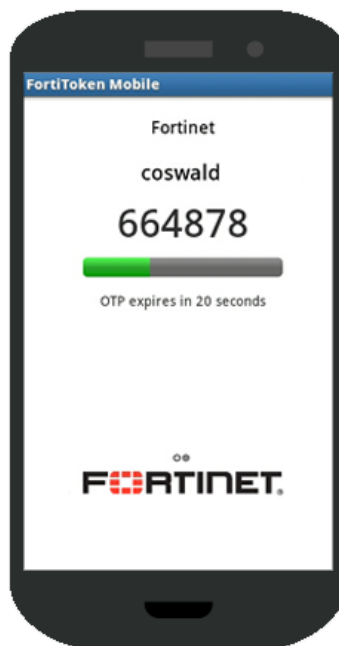
## 5. Setting up FortiToken Mobile on an Android device

Using your Android device, download and install **FortiToken Mobile**.

Open the app and add a new account. Select **Enter Manually**. Enter the activation code into FortiToken Mobile.



FortiToken Mobile can now generate a token for use with the FortiGate.



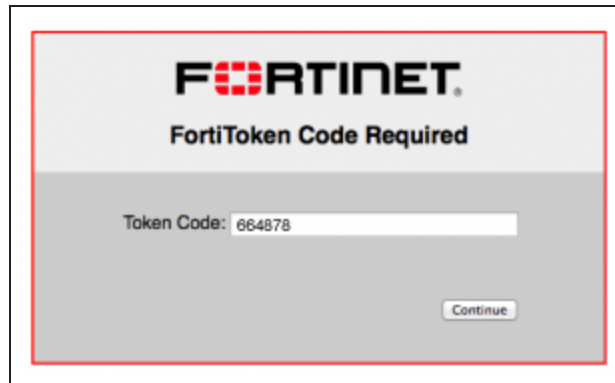
(Optional) For additional security, set a **PIN** for FortiToken Mobile using the app's **Settings** options.

## 6. Results

Attempt to browse the Internet. An authentication page will appear, requesting a **Username** and **Password**.

A screenshot of a web page titled 'FORTINET Authentication Required'. The page has a light gray background with a red border. It contains the Fortinet logo at the top, followed by the text 'Authentication Required'. Below this is a message: 'Please enter your username and password to continue.' There are two input fields: 'Username:' with the value 'coswald' and a small icon to the right, and 'Password:' with a masked value '\*\*\*\*\*' and a small icon to the right. A 'Continue' button is located at the bottom right of the form.

After the correct username and password are entered, a FortiToken code will be requested. Enter the code currently shown in the FortiToken Mobile app. Once the token is authenticated, you can connect to the Internet.

A screenshot of a web interface for FortiToken authentication. The top section has a light gray background with the 'FORTINET' logo in black and red, and the text 'FortiToken Code Required' in bold black. Below this is a darker gray section containing a text input field with the label 'Token Code:' and the value '664878'. A 'Continue' button is located at the bottom right of the input field area.

**FORTINET**  
**FortiToken Code Required**

Token Code: 664878

Continue

For further reading, check out [FortiToken](#) in the [FortiOS 5.2 Handbook](#).

# Security

This section contains information about using a FortiGate's security features, including antivirus, web filtering, application control, intrusion protection (IPS), email filtering, and data leak prevention (DLP). This section also includes information about using SSL inspection to inspect encrypted traffic.

## AntiVirus

- [FortiOS AntiVirus inspection modes](#)
- [AntiVirus with FortiSandbox](#)
- [Blocking Ultrasurf](#)

## Application Control

- [Blocking P2P traffic and YouTube applications](#)
- [Blocking Windows XP traffic](#)
- [Blocking and monitoring Tor traffic](#)
- [Controlling access to Apple's App Store](#)
- [Restricting online gaming to evenings](#)
- [Blocking Ultrasurf](#)

## Data Leak Prevention

- [Preventing data leaks](#)
- [Prevent credit card numbers from being leaked](#)

## Intrusion Protection

- [Protecting a web server](#)
- [Logging DNS domain lookups](#)

## SSL Inspection

- [Why you should use SSL inspection](#)
- [Preventing certificate warnings](#)
- [Exempting Google from SSL inspection](#)

## Web Filtering

- Blocking Facebook
- Blocking adult/mature content with Google SafeSearch
- Web rating overrides
- Web filtering using quotas
- Blocking Google access for consumer accounts
- Overriding a web filter profile
- Restricting online gaming to evenings
- Troubleshooting web filtering

# FortiOS AntiVirus inspection modes

If you include both FortiOS 5.0 and 5.2, there are three AntiVirus (AV) scanning inspection modes available. FortiOS 5.0 includes proxy and flow-based virus scanning. FortiOS 5.2 also uses proxy-based and flow-based scanning, but the flow-based mode in FortiOS 5.2 uses a new approach to flow-based scanning (that is sometimes called deepflow or deep flow scanning).

## AV Scanning 101

AntiVirus scanning examines files in HTTP, HTTPS, email, and FTP traffic for threats as they pass through your FortiGate unit. If the AV scanner finds a threat such as a virus or some other malware, FortiOS protects your network by blocking the file.

FortiOS includes a number of AntiVirus features that make virus scanning more user friendly. One of these features, called replacement messages, sends a customizable message to anyone whose file is blocked by AV scanning, to explain what happened and why. Other features make communication between the client and the server more seamless. The availability of these changes depending on the inspection mode.

## Proxy-based AV scanning

Proxy-based AV scanning is the most secure and feature-rich AV scanning mode. This mode uses a proxy to manage the communication between client and server. The proxy extracts content packets from the data stream as they arrive and buffers the content until the complete file is assembled. Once the file is whole, the AV scanner examines the file for threats. If no threats are found, the file is sent to its destination. If a threat is found, the file is blocked.

Because proxy-based scanning is applied to complete files it provides very effective threat detection. Proxy-based scanning also supports the a full range of features, including replacement messages and client comforting, making proxy-based scanning the most user friendly inspection mode. In addition the proxy manages the communication between the client and the server, so communication is cleaner.

Proxy-based scanning inspects all files under the oversized threshold. This threshold is 10 MB by default but can be reconfigured. Any files larger than the threshold are considered oversized and not inspected.

## Flow-based AV scanning

Although the name "flow-based scanning" is used in both FortiOS 5.0 and 5.2, the two different versions handle this mode in very different ways.

### Flow AV in FortiOS 5.0

In FortiOS 5.0, flow-based AV scanning scans the content of individual data packets as they pass through the FortiGate. There is no proxy involved so packets are not changed by the proxy and files are not buffered for

analysis. Potentially less memory and CPU resources are used, resulting in a potential performance increase compared to using proxy-based mode. FortiOS 5.0 flow-based AV scanning is also not limited by file size.

Flow AV uses the IPS engine and the AV database and is effective at many kinds of threat detection; however, because it can only analyze what is in an individual packet rather than a complete file, flow-based scanning cannot detect some types of malware, including polymorphic code. Malware in documents, compressed files, and some archives are also less likely to be detected.

Flow AV does not actually block files, it stops delivering the rest of the file once a threat has been detected. This means that parts of the file may already have been delivered when the threat has been detected and the recipient application is responsible for dealing with the partially complete content.

In addition flow AV can be less user friendly. Replacement messages are not supported and clients may have to wait for sessions to time out without knowing why content has been blocked.

## Flow AV in FortiOS 5.2 (deepflow or deep flow)

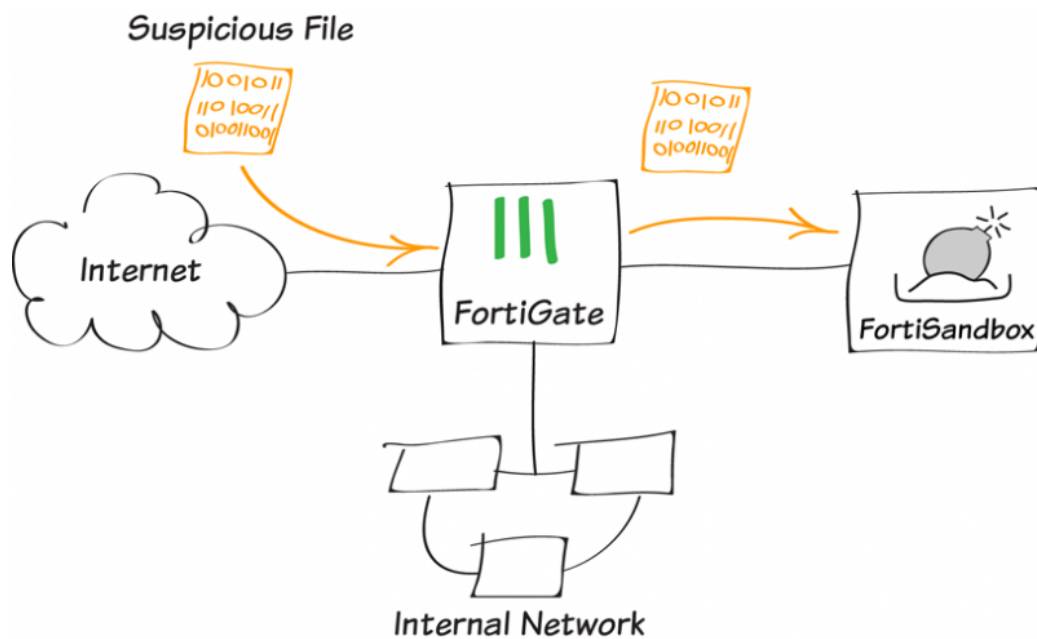
FortiOS 5.2 introduced a new type of flow-based AV scanning, that is sometimes called deepflow or deep flow, and that takes a hybrid approach where content packets are buffered while simultaneously being sent to their destination. When all of the files packets have been collected and buffered, but before the final packet is delivered, the buffered file is scanned. If a threat is found, the last packet is blocked and the client application has to deal with not getting the completed file. If no threat is found the final packet is sent and the user gets their file.

Deepflow AV scanning is as good as proxy-based AV scanning at detecting threats. There may be a small performance advantage over proxy-based AV as files get larger based on the difference between sending the whole file after analysis and just sending the last packet. Deepflow's most notable limitation is that, just like the flow-based AV in 5.0, it does not support many of the user-friendly features provided by proxy-based AV.

## The future of AV scanning

One of the current plans for FortiOS 5.4 is to add a new, "quick" mode for AV scanning.

# AntiVirus with FortiSandbox



In this recipe, you will apply antivirus scanning to your network traffic. Any suspicious files entering your network will be sent to a FortiSandbox for further examination.

This recipe was written using FortiSandbox 2.1.0.



# 1. Connecting the FortiSandbox

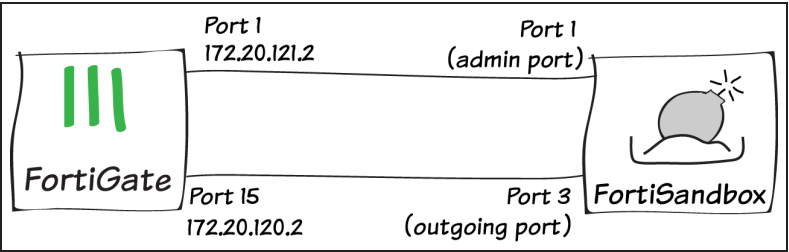
Connect the FortiSandbox to your FortiGate as shown in the diagram, so that port 1 and port 3 on the FortiSandbox are on different subnets.

Port 3 on the FortiSandbox is used for outgoing communication triggered by the execution of the files under analysis. It is recommended to connect this port to an isolated interface on your FortiGate (in the example, port 15), to protect the rest of the network from threats currently being investigated by the FortiSandbox.

The FortiSandbox requires Internet access on port 3. On the FortiGate, go to **Policy & Objects > Policy > IPv4** and create a policy allowing connections from the FortiSandbox to the Internet (using the isolated interface on the FortiGate mentioned above).

On the FortiSandbox, go to **System > Network > Static Routing** and add static routes for both port 1 and port 3.

The static route for port 3 must have the **Destination/IP Mask** `0.0.0.0/0.0.0.0`, while port 1 is assigned the **Destination/IP Mask** for traffic in the local network.



|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | port15          | + |
| Source Address      | all             | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | wan1            | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | Click to add... |   |
| Action              | ACCEPT          |   |

|                          | IP/Mask                | Gateway      | Device |
|--------------------------|------------------------|--------------|--------|
| <input type="checkbox"/> | 0.0.0.0/0.0.0.0        | 172.20.120.2 | port3  |
| <input type="checkbox"/> | 172.20.0.0/255.255.0.0 | 172.20.121.2 | port1  |

Once the FortiSandbox has access to the Internet through port 3, it will begin to activate the VM licenses.

Before continuing with this recipe, wait until a green arrow shows up beside **Windows VM** in the FortiSandbox's **System Information** widget, found at **System > Status**. This indicates that the VM activation process is complete.

| System Information       |  |
|--------------------------|--|
| HA-Cluster Status        | Standalone                                     |
| Host Name                | FSA1KD3A14000118 [Change]                      |
| Serial Number            | FSA1KD3A14000118                               |
| System Time              | Wed Aug 26 14:43:33 2015 EDT [Change]          |
| Firmware Version         | v2.10,build0081 (GA) [Update]                  |
| System Configuration     | Last Backup: 2015-08-25 16:58 [Backup/Restore] |
| System Utilities Version | 02001.00078 [Update]                           |
| Current Administrator    | admin  |
| Uptime                   | 0 day(s) 0 hour(s) 8 minute(s)                 |
| Windows VM               | ➔  |
| Microsoft Office         | ⚠ [Upload License]                             |
| VM Internet Access       | ➔  |
| FDN Download Server      | ➔  |
| Cloud Server             | ➔  |
| Web Filtering Server     | ➔  |
| Antivirus DB Contract    | N/A  |
| Web Filtering Contract   | N/A  |
| Shutdown / Reboot        | Reboot<br>Shutdown                             |

## 2. Enabling Sandbox Inspection

On the FortiGate, go to **System > Config > FortiSandbox**. Select **Enable Sandbox Inspection** and select **FortiSandbox Appliance**.

[tippy title="\*" class="myclass" showheader="false" width="auto" height="auto"]If you have a FortiCloud account, you can also select **FortiSandbox Cloud**.[/tippy]

Set the **IP Address** (in the example, *172.20.121.128*) and enter a **Notifier Email**, where notifications and reports will be sent.

After you select **Apply**, select **Test Connectivity**. The **Status** shows as **unreachable**, because the FortiGate has not been authorized to connect to the FortiSandbox.

**FortiSandbox Settings**

☒ Enable Sandbox Inspection

☒ FortiSandbox Appliance

IP Address

Notifier Email


**Test FortiSandbox Connectivity**

FortiSandbox Server

Status

On the FortiSandbox, go to **File-based Detection > File Input > Device**. Edit the entry for the FortiGate.

Under **Permissions**, enable **Authorized**.

| Device Status  |   |
|----------------|---|
| Serial Number: | FG100D3G12812324  |
| Alias:         | FG100D3G12812324  |
| IP:            | 172.20.121.46   |
| Status:        |  |
| Last Modified: | 2015-08-26 14:44:25   |
| Last Seen:     | 2015-08-26 14:46:56   |

| Permissions                      |  |
|----------------------------------|--|
| Authorized:                      | <input checked="" type="checkbox"/> Last Changed 2015-08-26 10:09:03 |
| New VDOMs Inherit Authorization: | <input checked="" type="checkbox"/>                                  |

On the FortiGate, go to **System > Config > FortiSandbox** and select **Test Connectivity**. The **Status** now shows that **Service is online**.

| Test FortiSandbox Connectivity |                    |
|--------------------------------|--------------------|
| FortiSandbox Server            | 172.20.121.128     |
| Status                         | Service is online. |

Return

### 3. Enabling FortiSandbox in the default AntiVirus profile

On the FortiGate, go to **Security Profiles > AntiVirus** and enable **Send Files to FortiSandbox for Inspection**.

The screenshot shows the configuration for the 'default' AntiVirus profile. The 'Name' field is 'default'. The 'Comments' field contains 'Scan files and block viruses.' with a character count of 29/255. Under 'Inspection Mode', 'Flow-based' is selected. Under 'Detect Viruses', 'Block' is selected. Two checkboxes are checked: 'Send Files to FortiSandbox for Inspection' and 'Detect Connections to Botnet C&C Servers'. At the bottom, 'Block' is selected over 'Monitor'.

### 4. Applying AntiVirus scanning to network traffic

On the FortiGate, go to **Policy & Objects > Policy > IPv4** and view the policy list.

If the **AV** column is not visible, right-click on the title row, select **AV**, and select **Apply**.

If any security policy does not have AntiVirus applied, highlight that policy to make the **None** option visible in the **AV** column. Select **None**, then use the **Select Profile** option to set the policy to use the **default** profile.

In order to ensure that AntiVirus is applied to encrypted traffic, you must also make sure that the **deep-inspection** profile is used for **SSL Inspection**.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).*

The screenshot shows a table of security policies. A context menu is open over the 'AV' column header, showing options: 'Edit AV Profile', 'Select Profile' (highlighted), 'Remove AV Profile', 'Cut AV Profile', 'Copy AV Profile', and 'Show References'. The table has columns: Seq.#, From, To, Action, NAT, AV, and SSL Inspection. Policy 1 (lan to wan1) has Action 'ACCEPT', NAT 'Enable', AV 'default', and SSL Inspection 'deep-inspection'. Policy 2 (wan1 to lan) has Action 'ACCEPT', NAT 'Enable', AV 'None', and SSL Inspection 'certificate-inspection'. Policy 3 (any to any) has Action 'DENY', NAT is empty, AV is empty, and SSL Inspection is empty.

| Seq.# | From | To   | Action   | NAT      | AV         | SSL Inspection         |
|-------|------|------|----------|----------|------------|------------------------|
| 1     | lan  | wan1 | ✓ ACCEPT | ✓ Enable | AV default | SSL deep-inspection    |
| 2     | wan1 | lan  | ✓ ACCEPT | ✓ Enable | None       | certificate-inspection |
| 3     | any  | any  | ⊘ DENY   |          |            |                        |

### 5. Results

If your FortiGate discovers a suspicious file, it will now be sent to the FortiSandbox. To view information about the files that have been sent on the FortiGate, go to **Status > FortiView > FortiSandbox** to see a list of files names and current status.

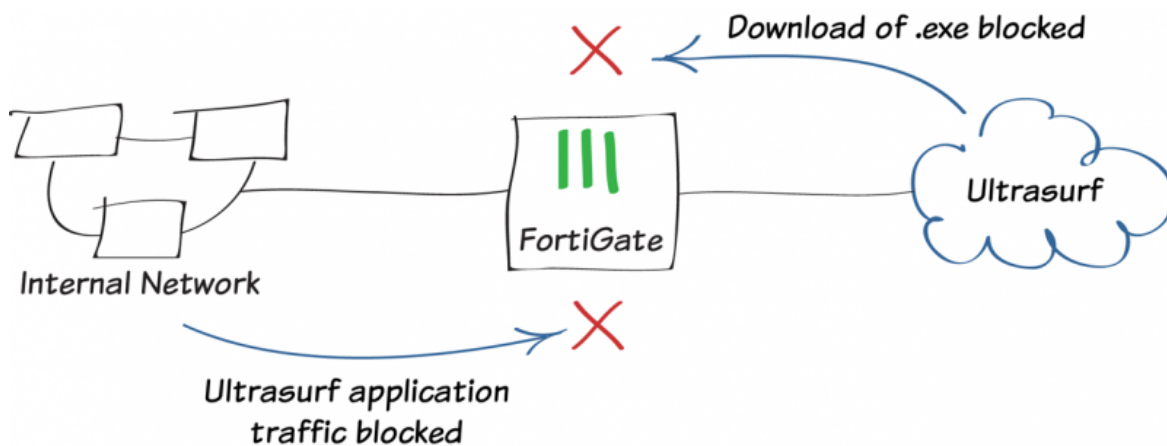
| Source          | File Name  | Status ▾ |
|-----------------|--|----------|
| 192.168.150.100 | boot.de09af735788b1a16a9918bafb639dbd9b6d5fe2.js | Clean    |
| 192.168.150.100 | card-be816c839a0614e1dbf66dfb59f4a15a.js         | Clean    |
| 192.168.150.100 | colorbox.css                                     | Clean    |
| 192.168.150.100 | comiccon_popexpo.css                             | Clean    |
| 192.168.150.100 | count.json                                       | Clean    |
| 192.168.150.100 | countdown.js                                     | Clean    |
| 192.168.150.100 | css  | Clean    |
| 192.168.150.100 | init.6749258e47fb0f4843de199ef85da0707436c238.js | Clean    |
| 192.168.150.100 | jquery-1.7.2.min.js                              | Clean    |
| 192.168.150.100 | jquery.carouFredSel-6.2.1.js                     | Clean    |
| 192.168.150.100 | jquery.colorbox-min.js                           | Clean    |
| 192.168.150.100 | jquery.maskedinput-1.2.2.js                      | Clean    |
| 192.168.150.100 | lightbox.js                                      | Clean    |
| 192.168.150.100 | main.js  | Clean    |
| 192.168.150.100 | modernizr-2.6.2.min.js                           | Clean    |
| 192.168.150.100 | scrollToTop.min.js                               | Clean    |
| 192.168.150.100 | sdk.js&version=v2.0                              | Clean    |
| 192.168.150.100 | slideshow.js                                     | Clean    |
| 192.168.150.100 | twitter_core.bundle.css                          | Clean    |
| 192.168.150.100 | vendor-2d48f8bce63f5e530dc817c7a2c2fbe1.js       | Clean    |

You can also view results on the FortiSandbox, by going to **System > Status** and viewing the **Scanning Statistics** widget.

*There may be a delay before results appear on the FortiSandbox.*

| Scanning Statistics - Last 24 Hours        |         |           |           |         |     |
|--|---------|-----------|-----------|---------|-----|
| Scanning Files Statistics in Last 24 Hours |         |           |           |         |     |
| Rating                                     | Sniffer | Device(s) | On Demand | Network | All |
| Malicious                                  | 0       | 0         | 0         | 0       | 0   |
| Suspicious - High Risk                     | 0       | 0         | 0         | 0       | 0   |
| Suspicious - Medium Risk                   | 0       | 0         | 0         | 0       | 0   |
| Suspicious - Low Risk                      | 0       | 0         | 0         | 0       | 0   |
| Clean                                      | 0       | 35        | 0         | 0       | 35  |
| Other                                      | 0       | 0         | 0         | 0       | 0   |
| Processed                                  | 0       | 35        | 0         | 0       | 35  |
| Pending                                    | 0       | 0         | 0         | 0       | 0   |
| Processing                                 | 0       | 0         | 0         | 0       | 0   |
| Total                                      | 0       | 35        | 0         | 0       | 35  |

# Blocking Ultrasurf

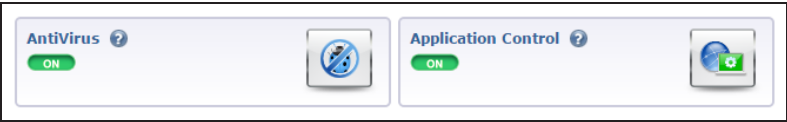


In this recipe, you will use antivirus scanning and application control to block network users from downloading and using Ultrasurf. As mentioned in a recent SysAdmin Note, Ultrasurf is an application that is used to bypass firewalls and browse the Internet anonymously.

In order to complete the final part of this recipe, download Ultrasurf before any security scanning is applied to your Internet traffic.

# 1. Enabling AntiVirus and Application Control

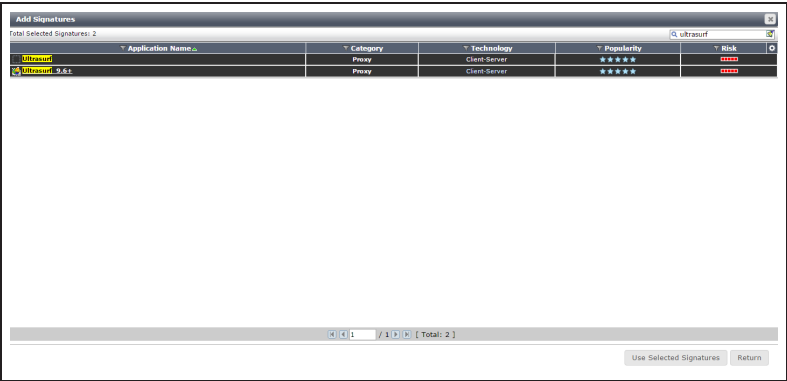
Go to **System > Config > Features** and make sure both **AntiVirus** and **Application Control** are enabled. If necessary, **Apply** your changes.



# 2. Editing the default Application Control profile

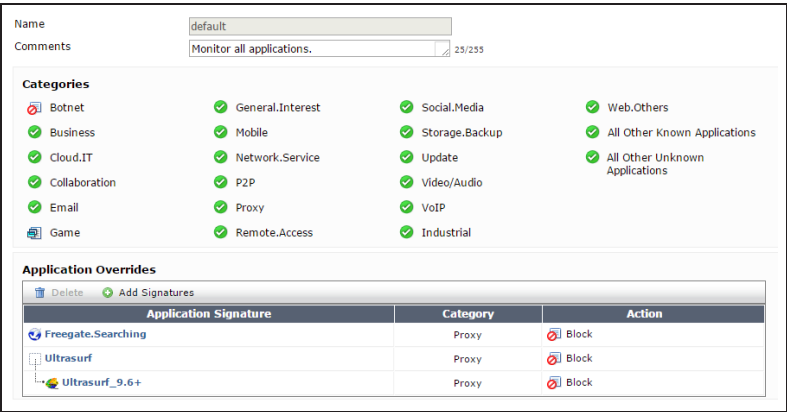
Go to **Security Profiles > Application Control** and edit the default profile. Under **Applications Override**, select **Add Signatures**.

Search for *ultrasurf*. Select the signatures, then select **Use Selected Signatures**.



The signatures will be added to the list, with **Action** set to block. You will also need to block the signature *Freemove.Searching*.

If you want to include all proxy applications, you can also choose to block the entire **Proxy** category.







### 3. Adding AntiVirus and Application Control profiles to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, enable both **AntiVirus** and **Application Control** and set both to use **default** profiles. Set **SSL/SSH Inspection** to **deep-inspection**.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#)*


| Security Profiles                      |   |
|--|---|
| <input checked="" type="checkbox"/> ON | AntiVirus <span>default</span>                   |
| <input type="checkbox"/> OFF           | Web Filter <span>default</span>                  |
| <input checked="" type="checkbox"/> ON | Application Control <span>default</span>         |
| <input checked="" type="checkbox"/> ON | SSL/SSH Inspection <span>deep-inspection</span>  |

### 4. Updating your AntiVirus and IPS definitions

Because Ultrasurf is constantly changing, it is recommended to update your AntiVirus and IPS definitions regularly, so that you can continue later versions of the application.

To set up regular updates, go to **System > Config > FortiGuard** and expand **AV & IPS Download Options**. Select an appropriate time for definitions to be downloaded.

You can also manually push an update by selecting **Update Now**.

|   |   |
|---|---|
| ▼ AV & IPS Download Options   |   |
| <input type="checkbox"/> Allow Push Update                         |   |
| <input type="checkbox"/> Use override push IP   | <input type="text" value="0.0.0.0"/> Port <input type="text" value="9443"/> |
| <input checked="" type="checkbox"/> Scheduled Update  | <input type="button" value="Update Now"/>                                   |
| <input type="radio"/> Every <input type="text" value="1"/> (hour)   |   |
| <input checked="" type="radio"/> Daily <input type="text" value="1"/> (hour)  |   |
| <input type="radio"/> Weekly <input type="text" value="Sunday"/> (day) <input type="text" value="1"/> (hour)  |   |
| <input checked="" type="checkbox"/> Submit attack characteristics to FortiGuard Service Network to help improve IPS signature quality (recommended) |   |



## 5. Results

Attempt to browse to [ultrasurf.us](http://ultrasurf.us). The page will not load.

On your FortiGate, go to **Log & Report > Traffic Log > Forward Traffic** and filter for **Destination IP: 65.49.14.131** (the IP of [ultrasurf.us](http://ultrasurf.us)). Traffic to this destination was blocked by the FortiGate.

| # | Date/Time | Source                        | Destination                 | Application Name | Security Action |
|---|-----------|-------------------------------|-----------------------------|------------------|-----------------|
| 1 | 13:35:28  | vickimartin (192.168.200.110) | 65.49.14.131 (ultrasurf.us) | Ultrasurf_9.6+   | Blocked         |
| 2 | 13:35:28  | vickimartin (192.168.200.110) | 65.49.14.131 (ultrasurf.us) | Ultrasurf_9.6+   | Blocked         |
| 3 | 13:35:23  | vickimartin (192.168.200.110) | 65.49.14.131 (ultrasurf.us) | Ultrasurf_9.6+   | Blocked         |
| 4 | 13:35:23  | vickimartin (192.168.200.110) | 65.49.14.131 (ultrasurf.us) | Ultrasurf_9.6+   | Blocked         |
| 5 | 13:35:15  | vickimartin (192.168.200.110) | 65.49.14.131 (ultrasurf.us) | Ultrasurf_9.6+   | Blocked         |

Attempt to download the Ultrasurf files from a third-party website, such as [Download.com](http://Download.com).

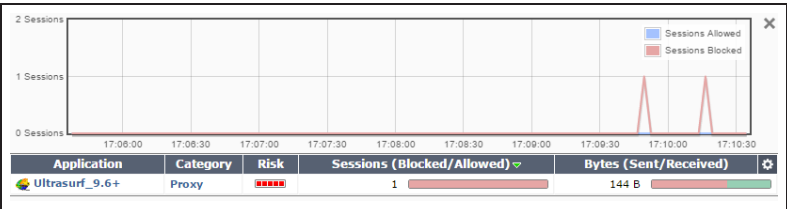
The download will be blocked.

*This result may vary based on which browser is being used. In the example, Firefox version 40.0.3 was used.*

**High Security Alert!!**  
  
You are not permitted to download the file "u-60070847.exe" because it is infected with the virus "Riskware/Agent".  
  
URL = [www.proinstall-download.com/download/?appid=75758651](http://www.proinstall-download.com/download/?appid=75758651)  
  
File quarantined as: .  
  
<http://www.fortinet.com/ve?vn=Riskware%2FAgent>

Attempt to use the copy of Ultrasurf you downloaded on your computer before starting this recipe. You will be unable to contact a server.

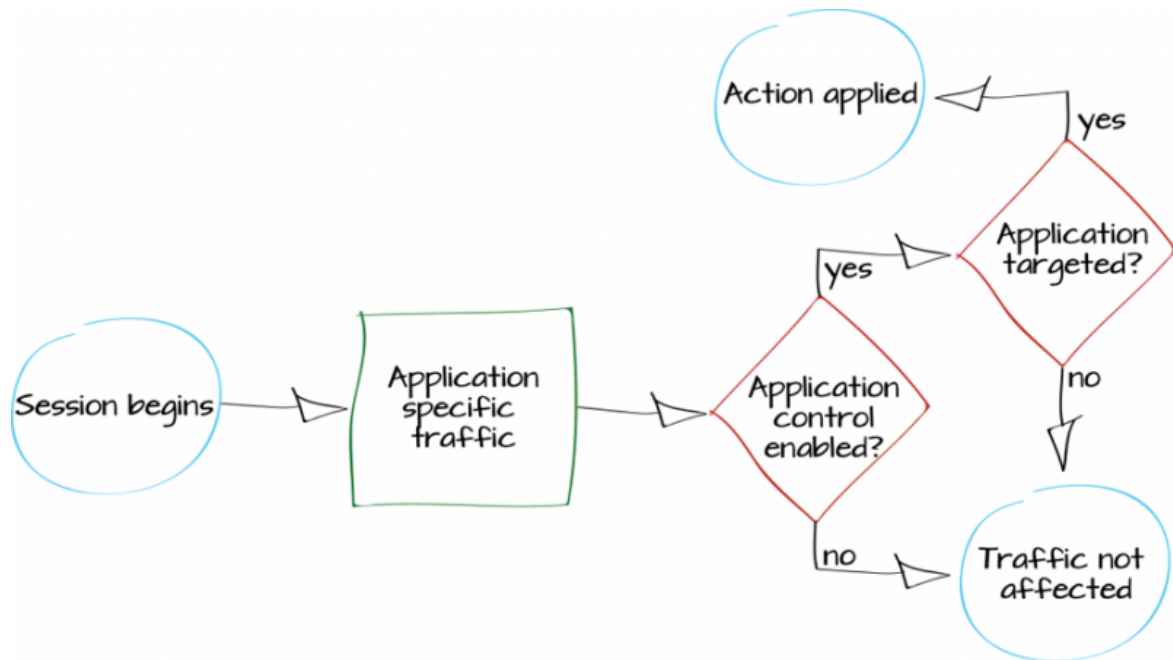
On your FortiGate, go to **System > FortiView > Applications > 5 minutes**, you will see that the FortiGate has blocked Ultrasurf.



*You may have to exit Ultrasurf in order to connect to your FortiGate.*

For further reading, check out [AntiVirus](#) and [Application control](#) in the [FortiOS 5.2 Handbook](#).

# Blocking P2P traffic and YouTube applications

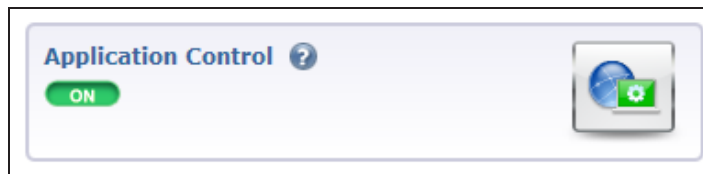


In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications cannot access the network.

A video of this recipe is available [here](#).

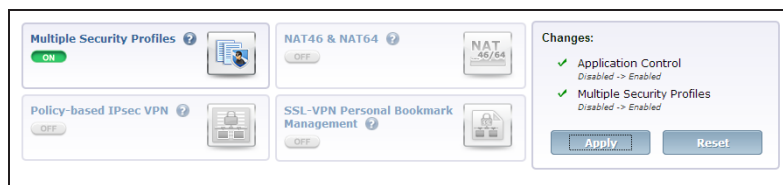
## 1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



Select **Show More** and enable **Multiple Security Profiles**.

Apply the changes.

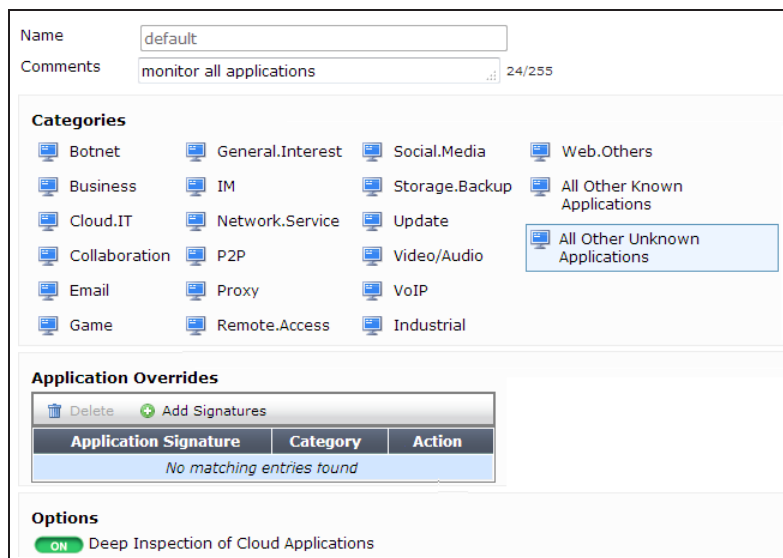


## 2. Using the default application profile to monitor network traffic

Go to **Security Profiles > Application Control** and view the **default** profile.

A list of application **Categories** is shown. By default, most categories are already set to **Monitor**. In order to monitor all applications, select **All Other Known Applications** and set it to **Monitor**. Do the same for **All Other Unknown Applications**.

The default profile also has Deep Inspection of Cloud Applications turned ON. This allows web-based applications, such as video streaming, to be monitored by your FortiGate.



### 3. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).*

|  |                                     |   |
|--|-------------------------------------|---|
| Incoming Interface   | internal                            | + |
| Source Address   | all                                 | + |
| Source User(s)   | Click to add...                     |   |
| Source Device Type   | Click to add...                     |   |
| Outgoing Interface   | wan1                                | + |
| Destination Address  | all                                 | + |
| Schedule   | always                              |   |
| Service  | ALL                                 | + |
| Action   | ACCEPT                              |   |
| <b>Firewall / Network Options</b>                                  |                                     |   |
| <input checked="" type="checkbox"/> NAT                            |                                     |   |
| <input checked="" type="radio"/> Use Destination Interface Address | <input type="checkbox"/> Fixed Port |   |
| <input type="radio"/> Use Dynamic IP Pool                          | Click to add...                     |   |
| <b>Security Profiles</b>   |                                     |   |
| <input type="checkbox"/> AntiVirus                                 | default                             |   |
| <input type="checkbox"/> Web Filter                                | default                             |   |
| <input checked="" type="checkbox"/> Application Control            | default                             |   |
| <input type="checkbox"/> IPS                                       | default                             |   |
| <input checked="" type="checkbox"/> SSL Inspection                 | deep-inspection                     | + |

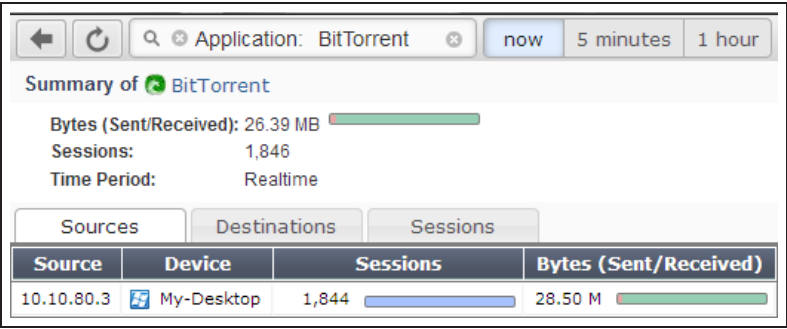
### 3. Reviewing the FortiView dashboards

Go to **System > FortiView > Applications** and select the **now** view.

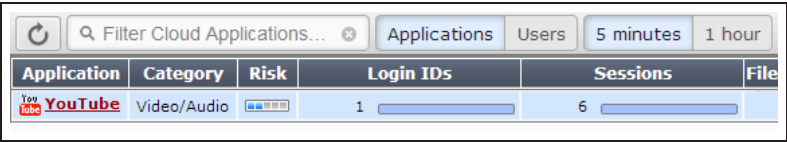
This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).

| Filter Applications... |                  |        |          |                       | now | 5 minutes | 1 hour |
|------------------------|------------------|--------|----------|-----------------------|-----|-----------|--------|
| Application            | Category         | Risk   | Sessions | Bytes (Sent/Received) |     |           |        |
| BitTorrent             | P2P              | High   | 78       | 410.37 K              |     |           |        |
| DNS                    | Network.Service  | Low    | 66       | 16.94 K               |     |           |        |
| SSL                    | Network.Service  | Low    | 21       | 16.04 M               |     |           |        |
| Skype                  | P2P              | Medium | 13       | 273.90 K              |     |           |        |
| Unknown                |                  |        | 6        | 442                   |     |           |        |
| Twitter                | Social.Media     | Low    | 3        | 29.61 K               |     |           |        |
| LastPass               | Storage.Backup   | Medium | 1        | 23.05 K               |     |           |        |
| Google.Plus            | Social.Media     | Low    | 1        | 17.78 K               |     |           |        |
| Dropbox                | Storage.Backup   | Medium | 1        | 340.18 K              |     |           |        |
| Jabber                 | Collaboration    | Medium | 1        | 19.87 K               |     |           |        |
| HTTP.Audio             | General.Interest | Low    | 1        | 33.38 M               |     |           |        |
| Facebook               | Social.Media     | Medium | 1        | 7.47 K                |     |           |        |

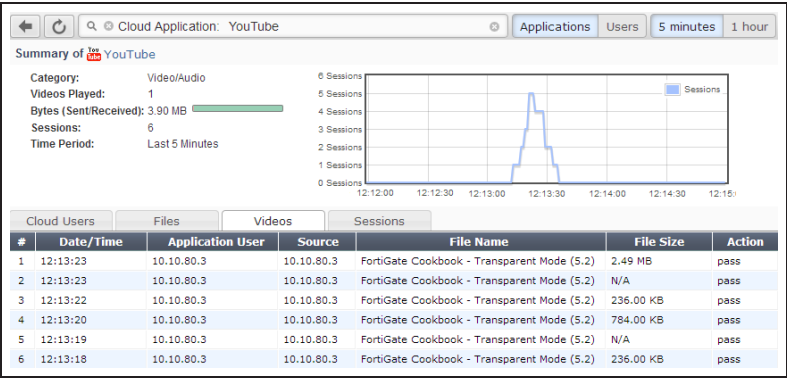
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



Similar information can be viewed for Cloud Applications by going to **System > FortiView > Cloud Applications** and selecting **Applications** that have been used in the last **5 Minutes**.



Cloud Applications also have drilldown options, including the ability to see which videos have been viewed if streaming video traffic was detected.



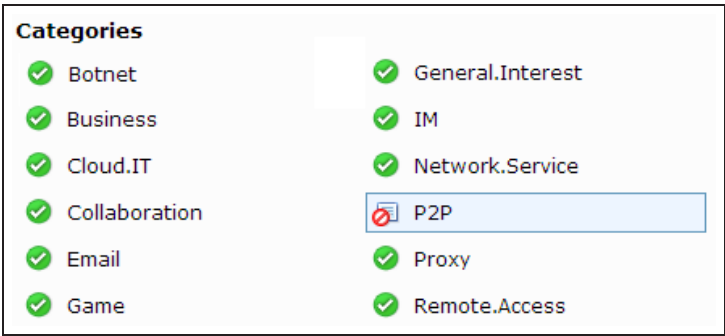
## 5. Creating an application profile to block applications

In the above example, traffic from BitTorrent, a Peer-to-Peer (P2P) downloading application, was detected. Now, you will create an application control profile that will block P2P traffic.

The new profile will also block all applications associated with YouTube, without blocking other applications in the **Video/Audio** category.

Go to **Security Profiles > Application Control** and create a new profile.

Select the **P2P** category and set it to **Block**.



Under **Application Overrides**, select **Add Signatures**.

**Search** for *Youtube* and select all the signatures that are shown.

Select **Use Selected Signatures**.

























| Application Name               | Category    | Technology    | Popularity | Risk |
|--------------------------------|-------------|---------------|------------|------|
| YouTube                        | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube.App                    | Video/Audio | Client-Server | ☆☆☆☆☆      | Low  |
| Youtube.Downloader.YTD         | Video/Audio | Client-Server | ☆☆☆☆☆      | Low  |
| YouTube_Comment.Posting        | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_HD.Streaming           | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Search.Safety.Mode.Off | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Search.Video           | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Video.Access           | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Video.Embedded         | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Video.Play             | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| YouTube_Video.Upload           | Video/Audio | Browser-Based | ☆☆☆☆☆      | Low  |
| Youtubeproxyfree               | Proxy       | Browser-Based | ☆☆☆☆☆      | High |

The signatures have been added to the Application Overrides list and have automatically been set to Block.

Enable **Deep Inspection of Cloud Applications**.

Delete

Add Signatures

| Application Signature  | Category    | Action  |
|--|-------------|---|
|  YouTube                        | Video/Audio |  Block |
|  YouTube.App                    | Video/Audio |  Block |
|  Youtube.Downloader.YTD         | Video/Audio |  Block |
|  YouTube_Comment.Posting        | Video/Audio |  Block |
|  YouTube_HD.Streaming           | Video/Audio |  Block |
|  YouTube_Search.Safety.Mode.Off | Video/Audio |  Block |
|  YouTube_Search.Video           | Video/Audio |  Block |
|  YouTube_Video.Access           | Video/Audio |  Block |
|  YouTube_Video.Embedded         | Video/Audio |  Block |
|  YouTube_Video.Play             | Video/Audio |  Block |
|  YouTube_Video.Upload           | Video/Audio |  Block |
|  Youtubeproxyfree               | Proxy       |  Block |

Options

ON

Deep Inspection of Cloud Applications

## 6. Adding the blocking profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Application Control** to use the new profile.

Security Profiles

ON

Antivirus

default

OFF

Web Filter

default

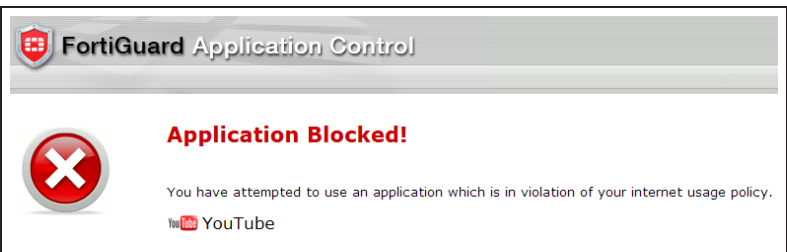
ON

Application Control

block-applications

# 7. Results

Attempt to browse to **YouTube**. A warning message will appear, stating that the application was blocked.



Traffic from BitTorrent applications will also be blocked.

To see information about this blocked traffic, go to **System > FortiView > All Sessions**, select the **5 minutes** view, and filter the traffic by application.

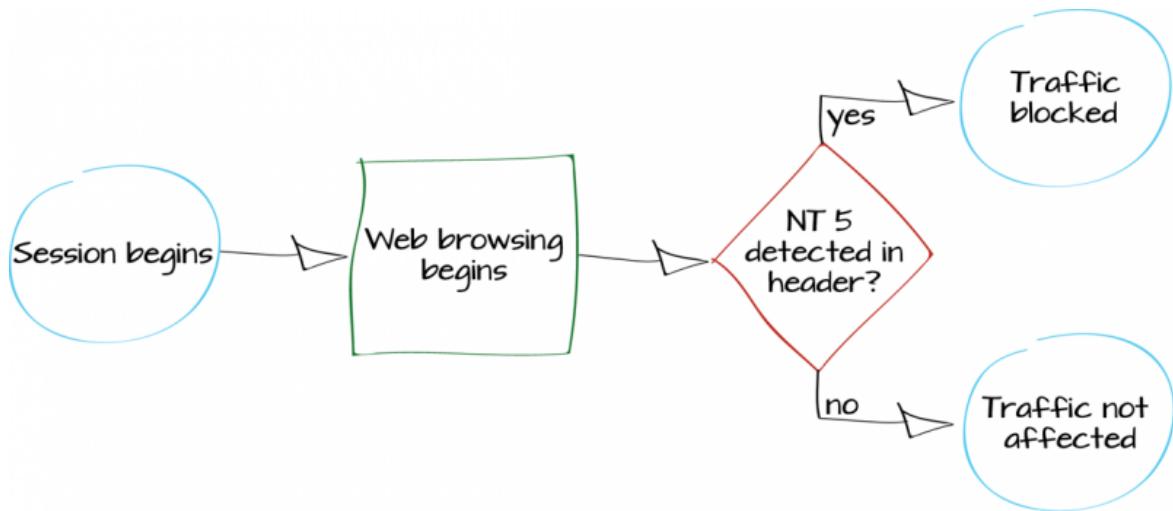
A screenshot of the FortiView 'All Sessions' table. The table has columns: #, Date/Time, Source, Device, Application Name, Security Action, and Security Events. The table is filtered by the application 'BitTorrent'. There are 11 rows of data, all showing 'Blocked' as the security action. The 'Security Events' column shows 'APP 1' for each row. The 'Date/Time' column shows times ranging from 14:08:30 to 14:09:33. The 'Source' column shows '10.10.80.3' for all entries. The 'Device' column shows 'My-Desktop' for all entries. The 'Application Name' column shows 'BitTorrent' for all entries. The 'Security Action' column shows 'Blocked' for all entries. The 'Security Events' column shows 'APP 1' for all entries.

| #  | Date/Time | Source     | Device     | Application Name | Security Action | Security Events |
|----|-----------|------------|------------|------------------|-----------------|-----------------|
| 1  | 14:09:33  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 2  | 14:09:26  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 3  | 14:09:19  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 4  | 14:09:16  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 5  | 14:09:12  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 6  | 14:09:05  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 7  | 14:08:58  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 8  | 14:08:51  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 9  | 14:08:44  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 10 | 14:08:37  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |
| 11 | 14:08:30  | 10.10.80.3 | My-Desktop | BitTorrent       | Blocked         | APP 1           |

For further reading, check out **Application control** in the **FortiOS 5.2 Handbook**.



# Blocking Windows XP traffic



In this example, you will use application control to block web traffic from PCs running Windows operating systems that NT 5, including Windows XP and Windows Server 2003 (includes Windows virtual machines).

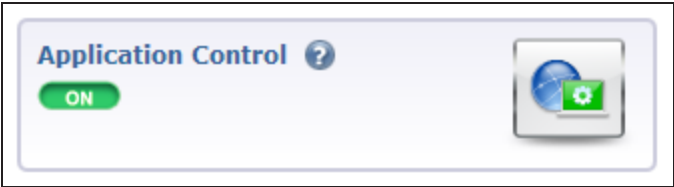
When a computer's operating system lacks vendor support, it becomes a threat to the network because newly discovered exploits will not be patched. Using the FortiGate application control feature, you can restrict these computers from accessing external resources.

*This recipe will only block web traffic from computers running the affected operating systems. If you wish to block these computers from being on the network entirely, further action will be necessary. However, the logs generated by this recipe can be used to identify the computers you wish to block.*

A video of this recipe is available [here](#).

# 1. Enabling Application Control

Go to **System > Config > Features**. Enable **Application Control** and **Apply** your changes.



# 2. Creating a custom application control signature






Go to **Security Profiles > Application Control** and select **View Application Signatures**.

Create a new signature with this syntax. (You can copy and paste this text into the **Signature** field.)

|           |   |
|-----------|---|
| Name      | <input type="text" value="Block-Windows-NT5"/>  |
| Comments  | <input type="text" value=""/> 0/255   |
| Signature | <pre>F-SBID( --attack_id 8151; --vuln_id 8151; --name "Windows.NT.5.Web.Surfing"; --default_action drop_session; --service HTTP; --protocol tcp; --app_cat 25; --flow from_client; --pattern "Windows NT 5."; --no_case; --context header; )</pre> <a href="#">Submit Signature</a> |

```
F-SBID( --attack_id 8151; --vuln_id 8151; --name "Windows.NT.5.Web.Surfing"; --default_action drop_session; --service HTTP; --protocol tcp; --app_cat 25; --flow from_client; --pattern "Windows NT 5."; --no_case; --context header; )
```

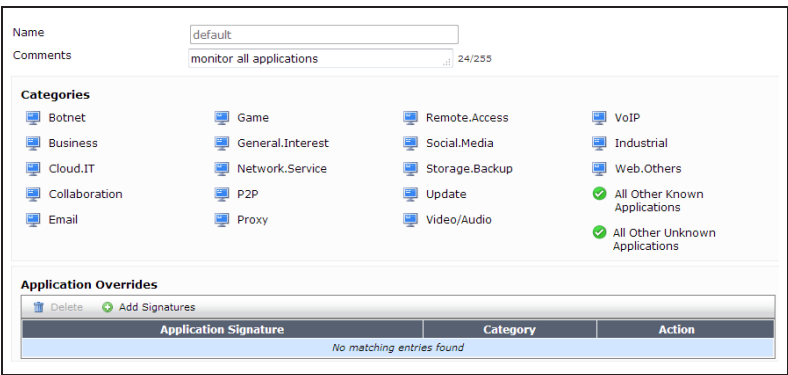
The signature will appear at the top of the application list and be listed in the **Web.Others** category.

| Application Name▲   | Category       |
|---|----------------|
|  Block-Windows-NT5 | Web.Others     |
|  0zz0              | Storage.Backup |
|  1and1             | Cloud.IT       |
|  1kxun             | Video/Audio    |
|  1und1.Mail        | Email          |

### 3. Adding the signature to the default Application Control profile

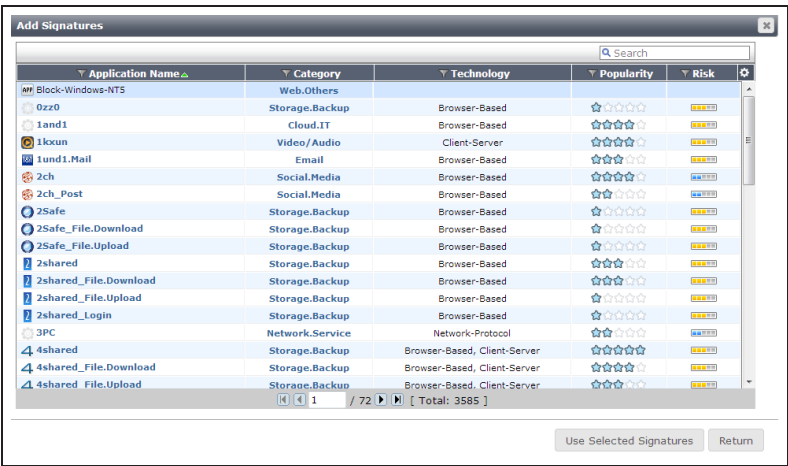
Go to **Security Profiles > Application Control** and edit the **default** policy.

Under **Application Overrides**, select **Add Signature**.



The new signature should appear at the top of the list. If it does not, search for the signature's name (in the example, *Block-Windows-NT5*).

Select the signature, then select **Use Selected Signatures**.



## 4. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Incoming Interface: internal  
Source Address: all  
Source User(s): Click to add...  
Source Device Type: Click to add...  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: always  
Service: ALL  
Action: ACCEPT

**Firewall / Network Options**  
☒ NAT  
☒ Use Outgoing Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool Click to add...

**Security Profiles**  
☐ AntiVirus default  
☐ Web Filter default  
☒ Application Control default

## 5. Results

When a PC running one of the affected operating systems attempts to connect to the Internet using a browser, a blocked message appears.

PCs running other operating systems, including later versions of Windows, are not affected.

**Application Blocked!**

You have attempted to use an application which is in violation of your internet usage policy.

Windows.NT.5.Web.Surfing

Category: Web.Others  
URL: http://google.ca/  
Client IP: 10.10.80.5  
Server IP: 24.156.131.108  
User name:  
Group name:  
Policy: e4769b60-bc02-51e3-73cd-93f99281538d  
FortiGate Hostname: FWF90D3Z13002661

Go to **System > FortiView > All Sessions** and select the **5 minutes** view.

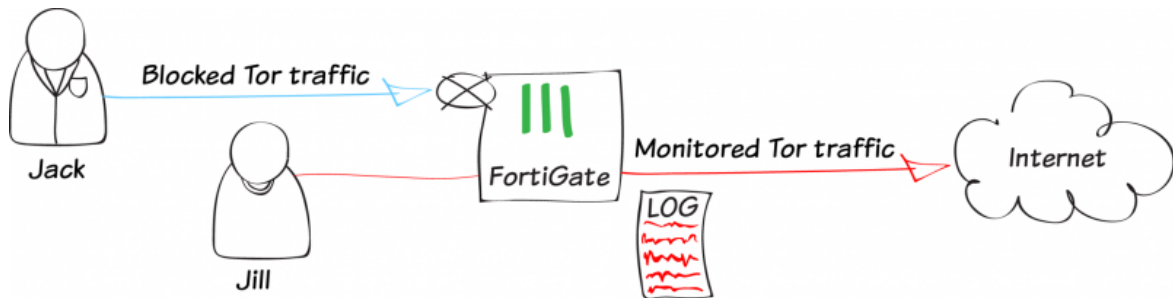
Filter the results to show sessions that were blocked.

| Date/Time | Source     | Device   | Destination                    | Application Name         | Security Action |
|-----------|------------|----------|--------------------------------|--------------------------|-----------------|
| 10:35:36  | 10.10.80.5 | Joscelin | 64.71.249.49 (www.youtube.com) | Windows.NT.5.Web.Surfing | block           |
| 10:35:31  | 10.10.80.5 | Joscelin | 24.156.131.108 (google.ca)     | Windows.NT.5.Web.Surfing | block           |
| 10:35:09  | 10.10.80.5 | Joscelin | 24.156.131.108 (google.ca)     | Windows.NT.5.Web.Surfing | block           |
| 10:34:34  | 10.10.80.5 | Joscelin | 208.91.114.28 (fortiguard.com) | Windows.NT.5.Web.Surfing | block           |

You will see that the Application Control signature, shown in the **Application Name** column, was used to block traffic from PCs running older Windows versions (in the example, the device **Joscelin**).

For further reading, check out **Custom Application & IPS Signatures** in the **FortiOS 5.2 Handbook**.

# Blocking and monitoring Tor traffic



In this recipe, you will allow one user to use the Tor browser application for web traffic, while monitoring the user's activity. Use of the Tor browser will be blocked for all other users.

The Tor browser allows users to bounce communication traffic around a distributed network of relays located around the world. For more information about Tor, check out the Fortinet blog entry [5 ½ Things To Know About The Tor Browser And Your Network](#).

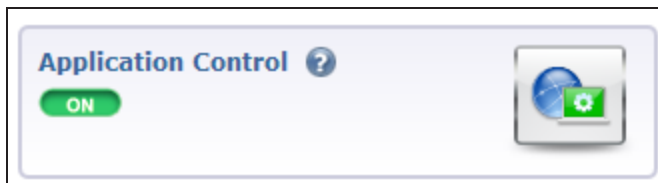
This recipe uses the default application control signatures for the Tor client and web-based Tor. These signatures will only match unmodified versions of the Tor application. Also, if a Tor session has already been established prior to connecting to the network, it may take up to 10 minutes before the FortiGate is able to monitor or block the traffic.

In this recipe, two user accounts, *jack* and *jill*, have already been configured. For more information about creating user accounts, see [User and device authentication](#).

A video of this recipe is available [here](#).

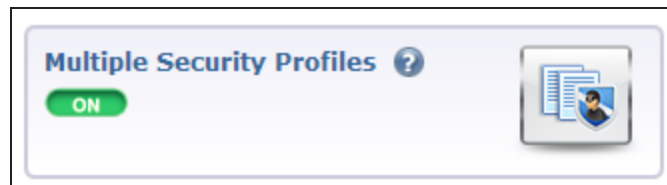
## 1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



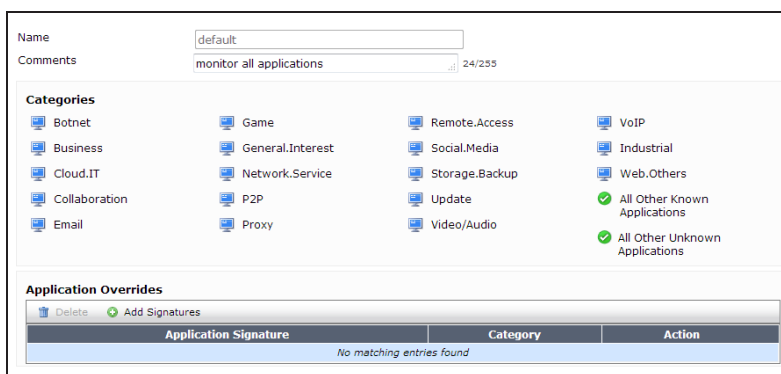
Select **Show More** and enable **Multiple Security Profiles**.

**Apply** the changes.



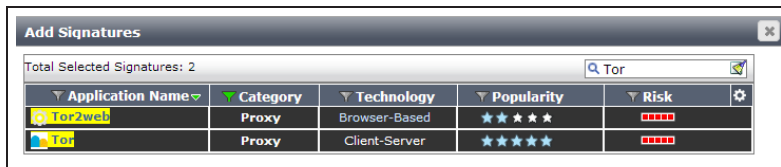
## 2. Blocking Tor traffic using the default profile

Go to **Security Profiles > Application Control** and edit the default profile.



Under **Application Overrides**, select **Add Signatures**.

Search for *Tor*, then filter the results to show only the **Proxy** category. Two signatures will appear: one for the Tor client and one for web-based Tor use.



Highlight both signatures, and select **Use Selected Signatures**.

Both signatures now appear in the **Application Overrides** list, with the **Action** set to **Block**.

| Application Overrides            |          |        |
|----------------------------------|----------|--------|
| <div>Delete Add Signatures</div> |          |        |
| Application Signature            | Category | Action |
| Tor                              | Proxy    | Block  |
| Tor2web                          | Proxy    | Block  |

### 3. Creating a profile that monitors Tor traffic

Go to **Security Profiles > Application Control** and create a new profile. Under **Application Overrides**, select **Add Signatures**.

| Application Overrides            |          |         |
|----------------------------------|----------|---------|
| <div>Delete Add Signatures</div> |          |         |
| Application Signature            | Category | Action  |
| Tor                              | Proxy    | Monitor |
| Tor2web                          | Proxy    | Monitor |

Search for and highlight both signatures, and select **Use Selected Signatures**.

In the **Application Overrides** list, double-click on the **Action** for each profile, and set it to **Monitor**.

### 4. Adding the application control profiles to your security policies

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet. Make sure the user *jack* is included in the **Source User(s)**.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Incoming Interface

lan

Source Address

all

Source User(s)

jack

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

 NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

 Antivirus

default

OFF

 Web Filter

default

ON

 Application Control

default



Create a second policy allowing connections from the internal network to the Internet. Set **Source User(s)** to *jill*.

Under **Security Profiles**, turn on **Application Control** and use the profile that will monitor Tor traffic.

Incoming Interface

lan

+

Source Address

all

+

Source User(s)

jill

×

+

Source Device Type

Click to add...

+

Outgoing Interface

wan1

+

Destination Address

all

+

Schedule

always

+

Service

ALL

+

Action

✓ ACCEPT

+

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

ON

Application Control

monitor-tor

+

Go to **Policy & Objects > Policy > IPv4** and view the policy list.

It is best to place more narrowly defined policies at the top of the list. In this case, the policy that monitors Tor is the most narrowly defined, because it is likely that less people will be using it than the policy that blocks Tor.

To rearrange the policies, select the column on the far left (in the example, **Seq.#**) and drag the policy to the desired position.

| Seq.# | From | To   | Source      | Destination | Action   | NAT    | Application Control | SSL Inspection             |
|-------|------|------|-------------|-------------|----------|--------|---------------------|----------------------------|
| 1     | lan  | wan1 | all<br>jill | all         | ✓ ACCEPT | Enable | APP monitor-tor     | SSL certificate-inspection |
| 2     | lan  | wan1 | all<br>jack | all         | ✓ ACCEPT | Enable | APP default         | SSL certificate-inspection |

## 5. Results

The Tor browser cannot be used for user authentication, so use a different browser to authenticate using *jill*'s credentials.

Browse the Internet using the Tor browser. You will be able to connect to the Internet.

Go to **System > FortiView > Applications** and select the **now** view. You will see a listing for the **Tor** traffic.

| Application | Category        | Risk | Sessions | Bytes (Sent/Received) |
|-------------|-----------------|------|----------|-----------------------|
| Skype       | Collaboration   | Low  | 38       | 38.74 KB              |
| DNS         | Network.Service | Low  | 29       | 7.15 KB               |
| UDP/40005   | Unknown         |      | 7        | 2.62 KB               |
| UDP/40021   | Unknown         |      | 5        | 1.91 KB               |
| UDP/40001   | Unknown         |      | 5        | 1.18 KB               |
| Tor         | Proxy           | High | 4        | 1.82 MB               |

If you double-click on the listing, you can view more information about this traffic, including detailed information on the sessions.

| Source            | Device     | Source Interface | Destination     | Destination Interface | Application | Bytes (Sent/Received) |
|-------------------|------------|------------------|-----------------|-----------------------|-------------|-----------------------|
| jill (10.10.80.3) | My-Desktop | lan              | 37.187.99.193   | wan1                  | Tor         | 14.37 KB              |
| jill (10.10.80.3) | My-Desktop | lan              | 37.252.190.133  | wan1                  | Tor         | 1.96 MB               |
| jill (10.10.80.3) | My-Desktop | lan              | 148.251.113.230 | wan1                  | Tor         | 7.83 KB               |

Go to **User & Device > Monitor > Firewall**. Select the *jill* account and select **De-authenticate**.



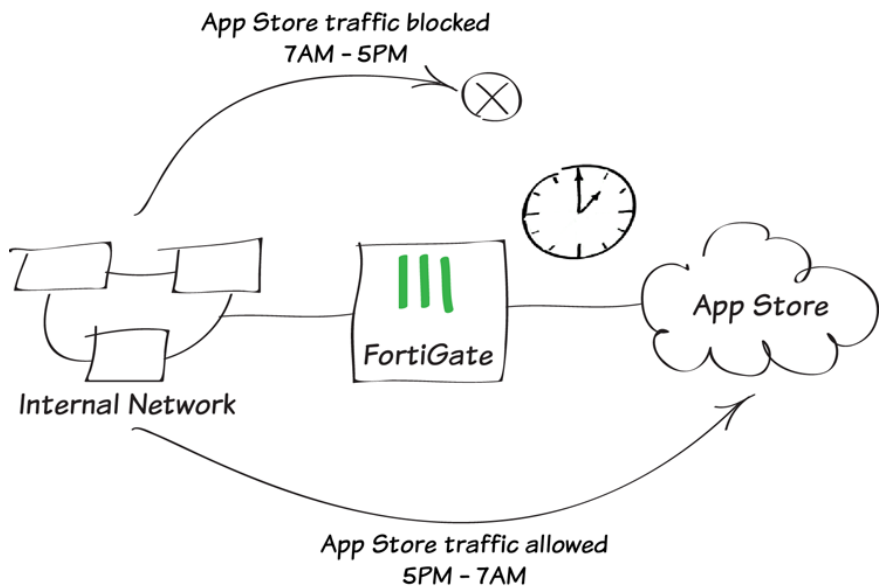
Authenticate using *jack*'s credentials. The Tor browser will be blocked.

Go to **System > FortiView > Applications** and select the **now** view. You will see that **Tor** traffic has been blocked.

| Application | Category        | Risk | Sessions (Blocked/Allowed) | Bytes (Sent/Received) |
|-------------|-----------------|------|----------------------------|-----------------------|
| DNS         | Network.Service | Low  | 22                         | 6.62 KB               |
| Skype       | Collaboration   | Low  | 9                          | 13.71 KB              |
| Tor         | Proxy           | High | 1                          | 476 B                 |

For further reading, check out [Application control](#) in the [FortiOS 5.2 Handbook](#).

# Controlling access to Apple's App Store

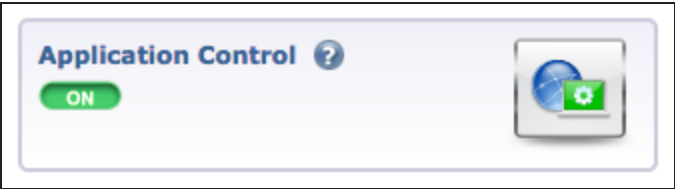


In this recipe, access to Apple's App Store is blocked between 7AM and 5PM. During the rest of the day, access is allowed.

This recipe applies to devices running MacOS and iOS devices (iPhone, iPad, or iPod).

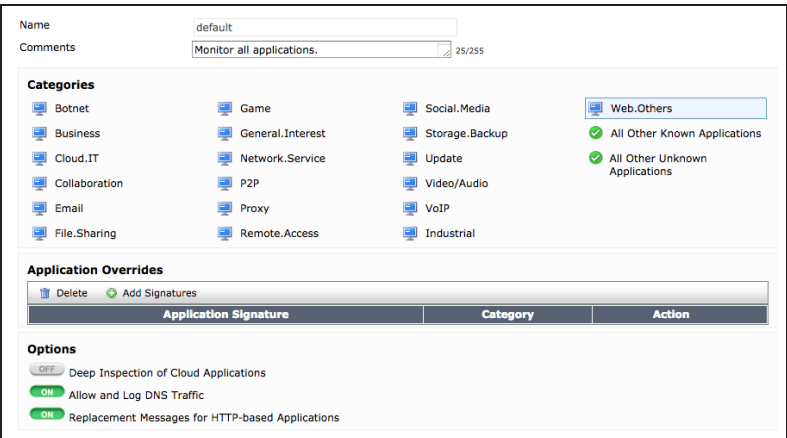
# 1. Enabling Application Control

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



# 2. Blocking the App Store

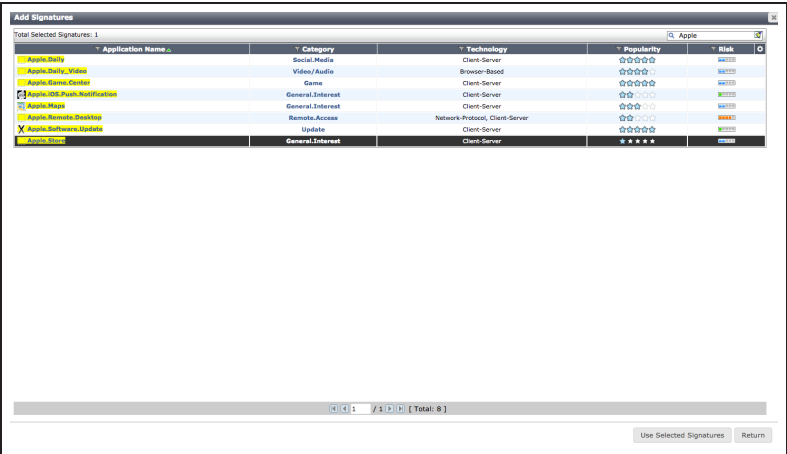
Go to **Security Profiles > Application Control** and edit the default profile.






Under **Application Overrides**, select **Add Signatures**.

Search for *Apple*. Highlight the **Apple.Store** signature, then select **Use Selected Signatures**.

If you wish to restrict updates from the App Store, you should also select the **Apple.Software.Update** signature.



The signature now appear in the **Application Overrides** list, with the **Action** set to **Block**.

| Application Overrides  |  |   |
|--|--|---|
|  Delete |  Add Signatures |   |
| Application Signature  | Category   | Action  |
| <input type="checkbox"/> Apple.Store   | General.Interest   |  Block |

### 3. Creating a schedule

Go to **Policy & Objects > Objects > Schedules** and create a new schedule.

Set **Type** to **Recurring**, select the appropriate **Days**, and set **Start Time** to 7AM (Hour 7, Minute 0) and **Stop Time** to 5PM (Hour 17, Minute 0).

Type

☒ Recurring ☐ One-time

Name

App-store-blocked

Days

☒ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

Start Time

Hour  Minute

Stop Time

Hour  Minute

### 4. Creating a security policy to block the App Store

Go to **Policy & Objects > Policy > IPv4** and create a new policy that allows connections from the internal network to the Internet.

Set **Schedule** to the new schedule.

Enable **Application Control** and set it to use the new profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).

Incoming Interface

lan

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

App-store-blocked

Service

ALL

Action

ACCEPT

Firewall / Network Options

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Security Profiles

☐ AntiVirus

☐ Web Filter

☒ Application Control

☐ IPS

☐ DLP Sensor

☒ SSL/SSH Inspection

## 5. Ordering the security policies

If you do not have a general policy that allows connections from the internal network to the Internet without blocking the App Store, you will need to create one before you can continue with this step.

Go to **Policy & Objects > Policy > IPv4** and view your **lan - wan1** policies.

In the example, the general policy allowing Internet access appears first in the list, followed by the new policy that blocks the App Store. To make sure the App Store is blocked, you must re-order the policies so that the new policy is higher on the list.

To rearrange the policies, select the column on the far left (in the example, **Seq.#**) and drag the policy to its new position.

| Seq.#              | Source | Destination | Schedule          | Service | Action   | NAT    | Application Control | SSL Inspection  | Log   |
|--------------------|--------|-------------|-------------------|---------|----------|--------|---------------------|-----------------|-------|
| lan - wan1 (1 - 2) |        |             |                   |         |          |        |                     |                 |       |
| 1                  | all    | all         | always            | ALL     | ✓ ACCEPT | Enable |                     |                 | ✓ All |
| 2                  | all    | all         | App-store-blocked | ALL     | ✓ ACCEPT | Enable | App default         | deep-inspection | UTM   |

| Seq.#              | Source | Destination | Schedule          | Service | Action   | NAT    | Application Control | SSL Inspection  | Log   |
|--------------------|--------|-------------|-------------------|---------|----------|--------|---------------------|-----------------|-------|
| lan - wan1 (1 - 2) |        |             |                   |         |          |        |                     |                 |       |
| 2                  | all    | all         | App-store-blocked | ALL     | ✓ ACCEPT | Enable | App default         | deep-inspection | UTM   |
| 1                  | all    | all         | always            | ALL     | ✓ ACCEPT | Enable |                     |                 | ✓ All |

## 6. Enforcing the schedule

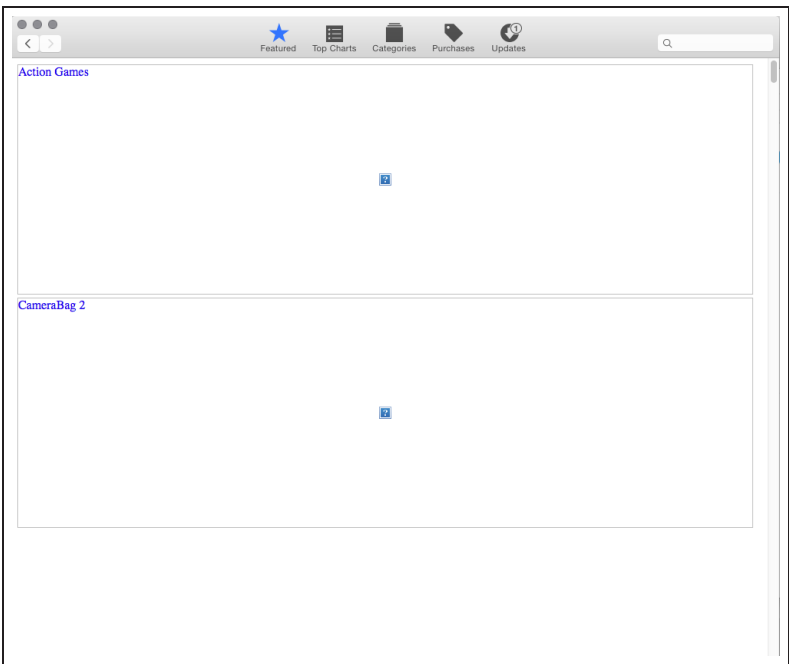
Go to **System > Dashboard > Status Console**, substituting the correct Policy ID for the new policy.

This ensures that the App Store is consistently blocked between 7AM and 5PM, even for sessions that start before 7AM.

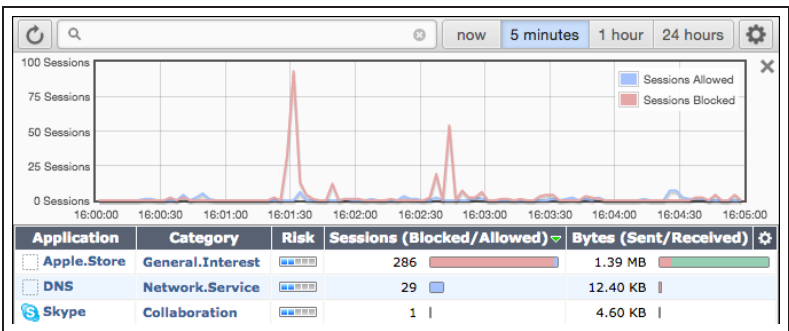
```
config firewall policy
edit <policy-id>
set schedule-timeout enable
end
end
```

# 7. Results

On a Mac or iOS device, attempt to run the App Store application between 7AM and 5PM. The application will not be able to fully load and no new apps can be downloaded.



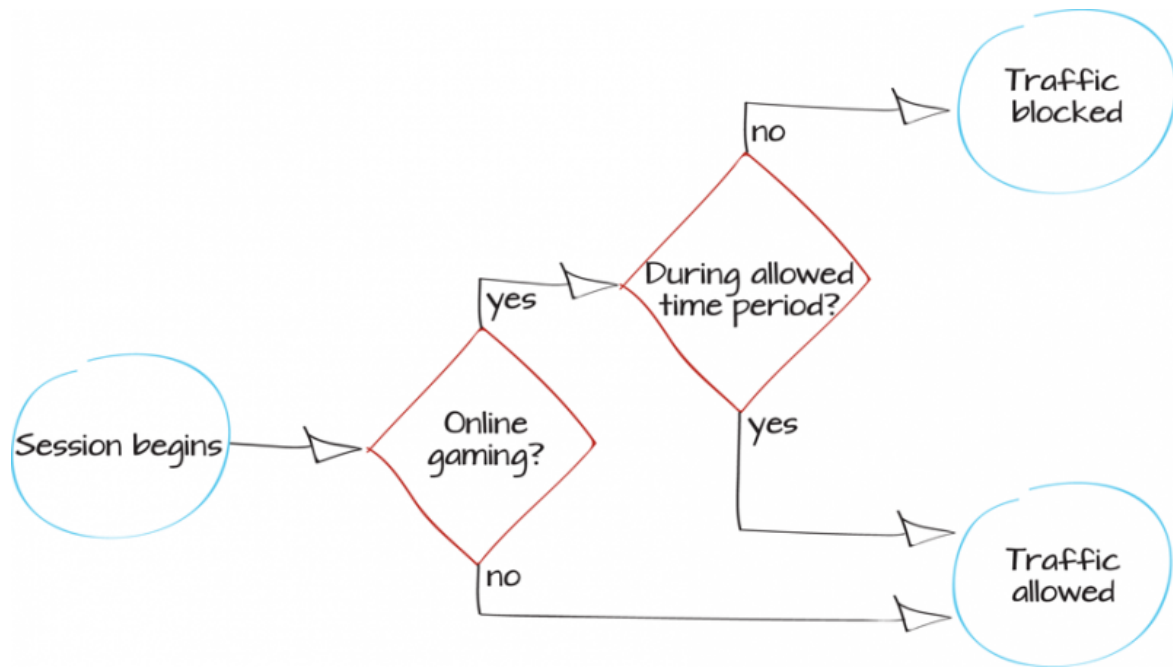
You can find information about the blocked traffic by going to **System > FortiView > Applications** and selecting the **5 minutes** view.



After 5PM, you will be able to connect to the App Store.

For further reading, check out [Application control](#) in the [FortiOS 5.2 Handbook](#).

# Restricting online gaming to evenings



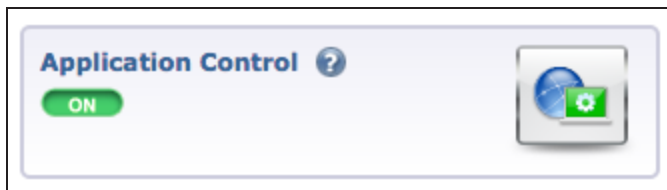
In this example, online gaming will only be allowed from 7-11PM. This includes gaming websites, applications, and consoles.

This example assumes that a general policy allowing connections from the internal network to the Internet has already been configured.

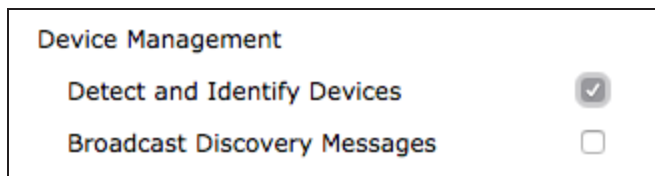


## 1. Enabling application control, web filtering, and device identification

Go to **System > Config > Features** and enable both **Application Control** and **Web Filter**. Apply your changes.



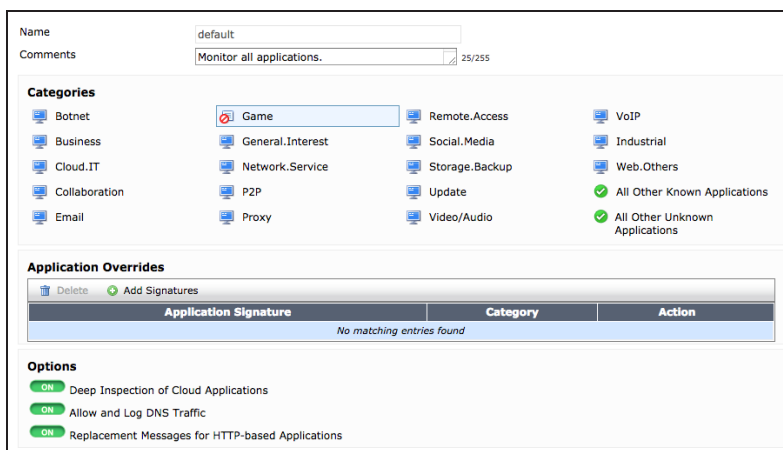
Go to **System > Network > Interfaces** and edit your **lan** interface.  
Enable **Detect and Identify Devices**.



## 2. Configuring application control and web filtering

Go to **Security Profiles > Application Control** and edit the **default** policy.

Under **Categories**, select **Game**, and set the category to **Block**.  
Under **Options**, enable **Deep Inspection of Cloud Applications**.



Go to **Security Profiles > Web Filter** and edit the **default** profile.

Enable **FortiGuard Categories**. Expand the **General Interest - Personal** category and select the sub-category **Games**. Set this sub-category to **Block**.

The screenshot shows the configuration page for the 'default' web filter profile. The 'Name' field is set to 'default' and the 'Comments' field contains 'Default web filtering.'. The 'Inspection Mode' is set to 'Proxy'. The 'FortiGuard Categories' checkbox is checked. A list of categories is displayed, with 'General Interest - Personal' expanded. Under this category, 'Games' is selected with a red 'X' icon, indicating it is blocked. Other categories like 'Advertising', 'Arts and Culture', etc., are marked with green checkmarks. A 'Quota on Categories with Monitor, Warning and Authenticate Actions' link is visible at the bottom.

Name: default

Comments: Default web filtering. 22/255

Inspection Mode: ☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show: All

- General Interest - Personal
  - Advertising
  - Arts and Culture
  - Brokerage and Trading
  - Child Education
  - Content Servers
  - Digital Postcards
  - Domain Parking
  - Dynamic Content
  - Education
  - Entertainment
  - Folklore
  - Games
  - Global Religion
  - Health and Wellness
  - Instant Messaging

Quota on Categories with Monitor, Warning and Authenticate Actions

### 3. Editing your general policy to block gaming

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Source Device Type** to all devices types that will be allowed on your network.

If you need to check the types of devices that are connecting to your network, go to **User & Device > Device > Device Definitions**. Do not include **Gaming Consoles**.

Under **Security Profiles**, enable both **Application Control** and **Web Filter** and set both to use to **default** profiles. Set **SSL/SSH Inspection** to **deep-inspection**.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).*

Incoming Interface: lan (VLAN ID: 0)  
Source Address: all  
Source User(s): Click to add...  
Source Device Type: Android Phone, Mac, iPad, Windows PC  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: always  
Service: ALL  
Action: ACCEPT

**Firewall / Network Options**  
☒ NAT  
• Use Outgoing Interface Address ☐ Fixed Port  
☐ Use Dynamic IP Pool  
  
☐ Compliant with FortiClient Profile

**Security Profiles**  
☐ AntiVirus: default  
☒ Web Filter: default  
☒ Application Control: default  
☐ DLP Sensor: default  
Proxy Options: default  
☒ SSL/SSH Inspection: deep-inspection

### 3. Creating a schedule for when gaming is allowed

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

Select all **Days** and set **Start Time** to **Hour 19 (7PM)** and **Stop Time** to **Hour 23 (11PM)**.

Type: ☒ Recurring ☐ One-time  
Name: gaming-allowed  
Days: ☒ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday  
Start Time: Hour 19 Minute 0  
Stop Time: Hour 23 Minute 0

## 4. Creating a policy that allows gaming between 7-11PM

Go to **Policy & Objects > Policy > IPv4** and create a new policy that will allow devices on the LAN to have Internet access.

Set **Schedule** to use the new schedule.

|                     |                  |   |
|---------------------|------------------|---|
| Incoming Interface  | lan (VLAN ID: 0) | + |
| Source Address      | all              | + |
| Source User(s)      | Click to add...  |   |
| Source Device Type  | Click to add...  |   |
| Outgoing Interface  | wan1             | + |
| Destination Address | all              | + |
| Schedule            | gaming-allowed   |   |
| Service             | ALL              | + |
| Action              | ACCEPT           |   |

Go to **System > Dashboard > Status** and enter the following in the CLI console, substituting the ID for the new policy.

```
config firewall policy
edit <policy_id>
set schedule-timeout enable
end
end
```

This will make sure that if someone is gaming during the allowed time, their session will be blocked after 11PM.

## 6. Ordering the policies

Go to **Policy & Objects > Policy > IPv4** and order the policies so that the general policy is located below the policy that allows gaming between 7-11PM.

| Seq.#              | Source        | Destination | Schedule       | Service | Action   | NAT    | Web Filter | Application Control | SSL Inspection  |
|--------------------|---------------|-------------|----------------|---------|----------|--------|------------|---------------------|-----------------|
| lan - wan1 (1 - 2) |               |             |                |         |          |        |            |                     |                 |
| 1                  | all           | all         | gaming-allowed | ALL     | ✓ ACCEPT | Enable |            |                     |                 |
| 2                  | all           | all         | always         | ALL     | ✓ ACCEPT | Enable | default    | default             | deep-inspection |
|                    | Android Phone |             |                |         |          |        |            |                     |                 |
|                    | Mac           |             |                |         |          |        |            |                     |                 |
|                    | iPad          |             |                |         |          |        |            |                     |                 |
|                    | Windows PC    |             |                |         |          |        |            |                     |                 |


# 7. Results

During the time that gaming is blocked, attempt to browse to a gaming website, such as **Yahoo Games**. The site is blocked.

Attempt to run an online gaming application, such Steam. The application will be unable to connect to the Internet.

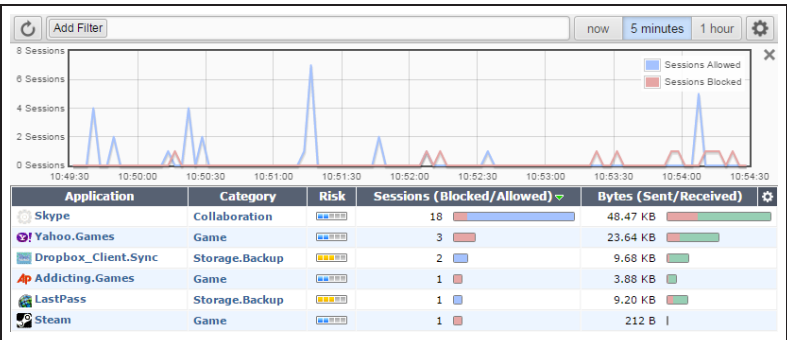
**Application Blocked!**

You have attempted to use an application which is in violation of your internet usage policy.

 **Yahoo.Games**

Category: Game  
URL: spdy://  
Client IP: 10.10.80.4  
Server IP: 98.139.199.204  
User name:  
Group name:  
Policy: e4769b60-bc02-51e3-73cd-93f99281538d  
FortiGate Hostname: FWF90D3Z13002661

To view information about this blocked traffic, go to **System > FortiView > Applications**.

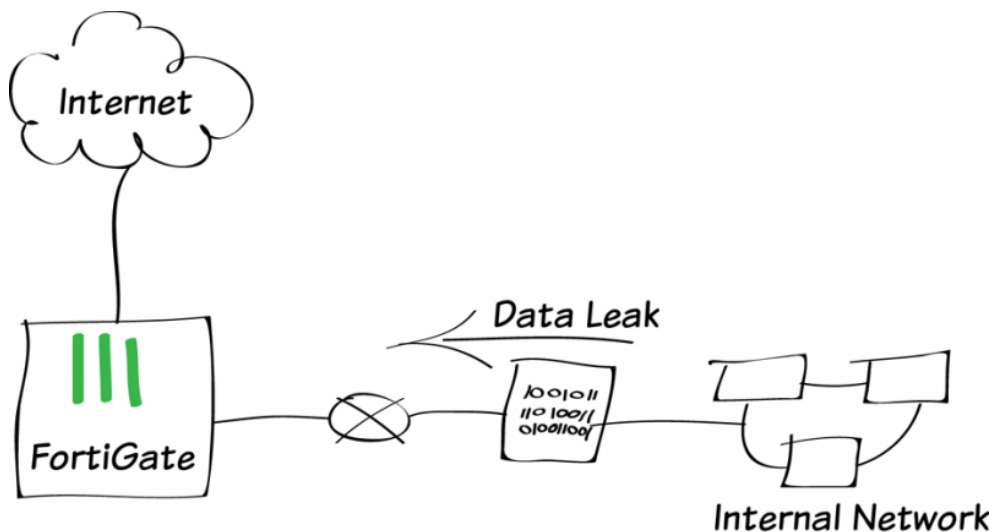


Attempt to connect to the Internet using a gaming console. The console will be unable to connect to the Internet.

Between 7-11PM, you are able to access the website, and all gaming applications and consoles can connect to the Internet.

For further reading, check out the **Security Profiles** in the **FortiOS 5.2 Handbook**.

# Preventing data leaks



In this example, you will block files that contain sensitive information from leaving your network. To do this, a Data Leak Prevention (DLP) profile will be used that blocks files that have a DLP watermark applied to them, as well as any .exe files.

A video of this recipe is available [here](#).

## 1. Enabling DLP and multiple security profiles

Go to **System > Config > Features** and ensure that **DLP** is turned **ON**.



Select **Show More** and ensure that **Multiple Security Profiles** is also turned **ON**. If necessary, **Apply** your changes.

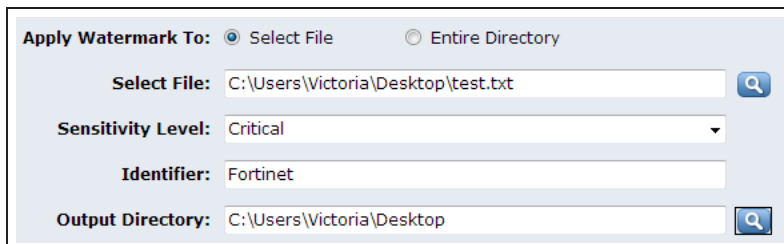


## 2. Applying a DLP watermark to a file

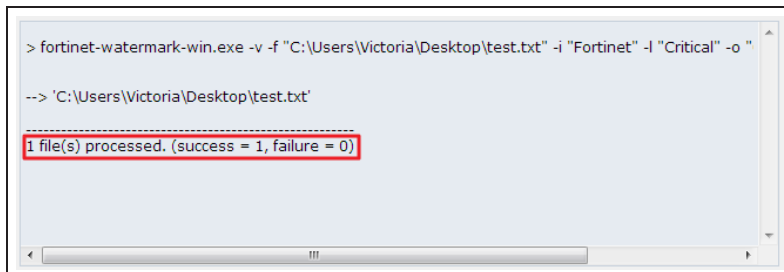
The DLP watermarking client is available as part of FortiExplorer. This feature is currently only available using FortiExplorer for Microsoft Windows.

If you do not already have FortiExplorer on your computer, click [here](#) to download it.

Open FortiExplorer. Under **Tools**, select **DLP Watermark**. Select **Apply Watermark to Select File**. Select the file and set the **Sensitivity Level**, **Identifier**, and **Output Directory**. Select **Apply Watermark**.



The dialogue box will show the file being processed. Ensure that the process was successful.



### 3. Creating a DLP profile

Go to **Security Profiles > Data Leak Prevention** and create a new profile.

Name:

Comment:  0/255

Create New

Edit Filter

Delete

| Seq #                     | Type | Action | Services | Archive |
|---------------------------|------|--------|----------|---------|
| No matching entries found |      |        |          |         |

In the Filter list, select **Create New**.

Set the filter to look for **Files**. Select **Watermark Sensitivity** and set it to match the watermark applied to the file. Do the same for **Corporate Identifier**.

Set **Examine the Following Services** to all the services required by your network.

Set **Action** to **Block**.

Filter

Messages

Files

Containing

Credit Card #

File Size >=

KB

Specify File Types

File Finger Print

Critical

Watermark Sensitivity:

Critical

Corporate Identifier:

Fortinet

Regular Expression

Encrypted

Examine the Following Services

Web Access

HTTP-POST

HTTP-GET

Email

SMTP

POP3

IMAP

MAPI

Others

FTP

NNTP

Action

Block

Create a second filter.

Set the filter to look for **Files**. Select **Specify File Types** and set **File Types** to **Executable (exe)**.

Set **Examine the Following Services** to all the services required by your network.

Set **Action** to **Block**.

Filter

Messages

Files

Containing

Credit Card #

File Size >=

KB

Specify File Types

File Types:

Executable (exe)

X

+

File Name Patterns:

Click to add...

File Finger Print

Critical

Watermark Sensitivity:

Critical

Corporate Identifier:

Regular Expression

Encrypted

Examine the Following Services

Web Access

HTTP-POST

HTTP-GET

Email

SMTP

POP3

IMAP

MAPI

Others

FTP

NNTP

Action

Block



Both filters now appear in the Filters list.

Name: block-sensitive-information

Comment: Comment0/255

Create New

Edit Filter

Delete

| Seq # | Type  | Action | Services                                   | Archive |
|-------|---|--------|--|---------|
| 1     | Watermark Sensitivity: Critical, Corporate Identifier: Fortinet | Block  | SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP | Disable |
| 2     | Specified File Types  | Block  | SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP | Disable |

#### 4. Adding the profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit your Internet-access policy.

Under **Security Profiles**, enable **DLP Sensor** and set it to use the new profile.

**SSL Inspection** is automatically enabled. Set it to use the **deep-inspection** profile to ensure that DLP is applied to encrypted traffic.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).*

Under **Logging Options**, enable **Log Allowed Traffic** and select **Security Events**.

Security Profiles

OFF

AntiVirus

OFF

Web Filter

OFF

Application Control

OFF

IPS

ON

DLP Sensor

ON

SSL Inspection

default

default

default

default

default

deep-inspection

Logging Options

ON

Log Allowed Traffic

Security Events

All Sessions

#### 5. Results

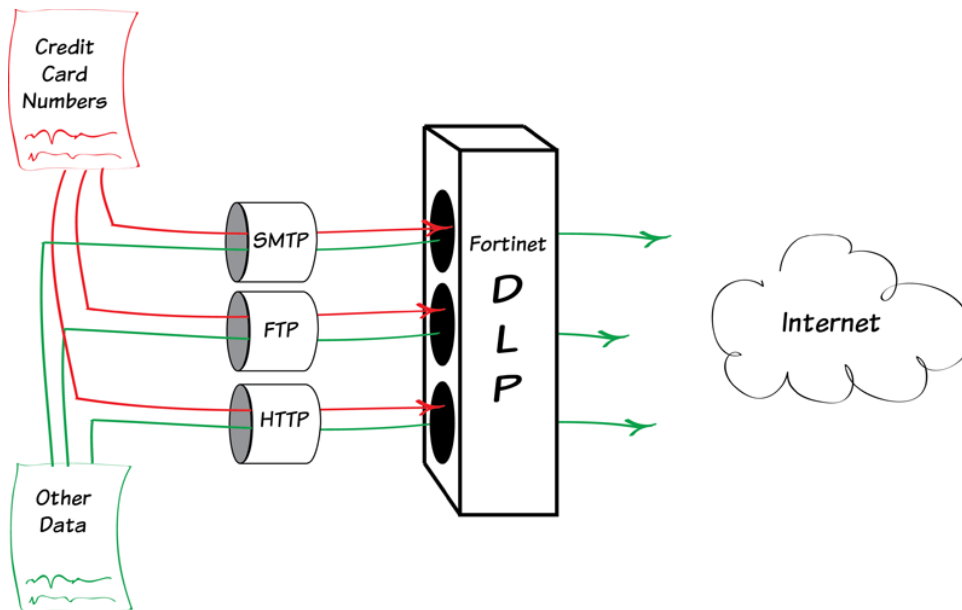
Attempt to send either the watermarked file or an .exe file using a protocol that the DLP filer is examining. Depending on which protocol is used, the attempt will either be blocked by the FortiGate or it will timeout.

Go to **System > FortiView > All Sessions** and select the **5 minutes** view for information about the blocked session.

| <div><div><div></div></div><div>Filter Sessions...</div><div><div></div></div></div> <div><div>now</div><div>5 minutes</div><div>1 hour</div></div> |           |            |                  |                 |                 |
|---|-----------|------------|------------------|-----------------|-----------------|
| #   | Date/Time | Source     | Application Name | Security Action | Security Events |
| 1   | 11:49:42  | 10.10.80.3 | HTTPS            | Blocked         | 1               |
| 2   | 11:48:32  | 10.10.80.3 | Unknown          |                 |                 |
| 3   | 11:48:32  | 10.10.80.3 | Unknown          |                 |                 |
| 4   | 11:48:32  | 10.10.80.3 | Unknown          |                 |                 |

For further reading, check out [Data leak prevention](#) in the [FortiOS 5.2 Handbook](#).

# Prevent credit card numbers from being leaked



In this example, you will use DLP to prevent credit card numbers from being sent out of your network using HTTP, FTP, or SMTP.

## 1. Enabling DLP

Go to **System > Config > Features** and make sure that **DLP** is turned **ON**.



## 2. Adding two filters to the default DLP sensor

Go to **Security Profiles > Data Leak Prevention** and edit the default sensor. Select **Create New** to add a new filter.

The first filter blocks web pages and email **Messages** containing credit card numbers.

A screenshot of the 'New Filter' dialog box. Under the 'Filter' section, 'Messages' is selected. The 'Containing' option is chosen with a dropdown menu showing 'Credit Card #'. Under 'Examine the Following Services', 'Web Access' has 'HTTP-POST' checked, and 'Email' has 'SMTP', 'POP3', and 'IMAP' checked. The 'Action' dropdown is set to 'Block'. 'OK' and 'Cancel' buttons are at the bottom right.

The second filter blocks **Files** containing credit card numbers. This includes email attachments and files uploaded with a web browser or using FTP.

A screenshot of the 'New Filter' dialog box. Under the 'Filter' section, 'Files' is selected. The 'Containing' option is chosen with a dropdown menu showing 'Credit Card #'. Other options like 'File Size', 'Specify File Types', 'File Finger Print', 'Watermark Sensitivity', 'Regular Expression', and 'Encrypted' are also visible. Under 'Examine the Following Services', 'Web Access' has 'HTTP-POST' and 'HTTP-GET' checked, 'Email' has 'SMTP', 'POP3', and 'IMAP' checked, and 'Others' has 'FTP' checked. The 'Action' dropdown is set to 'Block'. 'OK' and 'Cancel' buttons are at the bottom right.

Both filters appear in the default sensor.

Name: default

Comment: Log a summary of email and web traffic. 39/255

Create New Edit Filter Delete

| Seq # | Type                   | Action | Services                                   | Archive |
|-------|------------------------|--------|--|---------|
| 1     | Containing Credit Card | Block  | SMTP, POP3, IMAP, HTTP-POST                | Disable |
| 2     | Containing Credit Card | Block  | SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP | Disable |

### 3. Adding the new DLP sensor to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network (in this case connected to the **lan** interface) to the Internet.

Under **Security Profiles**, turn on **DLP Sensor** and use the **default** sensor. Set **SSL/SSH Inspection** to **deep-inspection**.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).*

Incoming Interface

lan (VLAN ID: 0)

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

ON

DLP Sensor

default

Proxy Options

default

ON

SSL/SSH Inspection

deep-inspection

### 4. Results

Locate some example credit card numbers to use for testing purposes. These can be found from a variety of locations, including [PayPal](#).

**Testing HTTP:** Go to a website with a comment section and attempt to post an example credit card number. The comment is blocked.

**Testing FTP:** Transfer a file containing an example credit card number using FTP. This transfer is blocked.

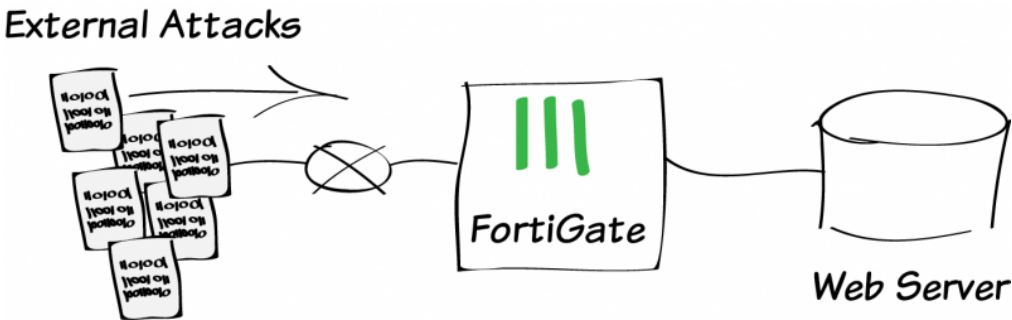
**Testing SNMP:** Send an email containing an example credit card number using a SNMP email client. This email is blocked.

To view more information about the blocked traffic, go to **Log & Report > Traffic Log > Forward Traffic** and filter for **Security Actions: Blocked**.

| Security Action: Blocked <span>Add Filter</span> |   |                  |                 |                 |
|--|---|------------------|-----------------|-----------------|
| Date/Time  | Destination   | Application Name | Security Action | Security Events |
| 04-22 16:53                                      | 213.180.204.25 (mail.yandex.com)                                      | HTTPS            | Blocked         | 2               |
| 04-22 16:53                                      | 213.180.204.25 (mail.yandex.com)                                      | HTTPS            | Blocked         | 3               |
| 04-22 16:51                                      | 23.195.216.135  | HTTP             | Blocked         | 1               |
| 04-15 16:20                                      | 208.91.113.212 (mail.fortinet-us.com)                                 | TCP/587          | Blocked         | 1               |
| 04-15 16:15                                      | 208.91.113.212 (mail.fortinet-us.com)                                 | TCP/587          | Blocked         | 1               |
| 04-15 15:49                                      | 66.111.4.148  | HTTPS            | Blocked         | 41              |
| 04-15 15:46                                      | 208.91.113.212 (mail.fortinet-us.com)                                 | TCP/587          | Blocked         | 1               |
| 04-15 15:45                                      | 208.91.113.212 (mail.fortinet-us.com)                                 | TCP/587          | Blocked         | 1               |
| 04-15 15:45                                      | 208.91.113.212 (mail.fortinet-us.com)                                 | TCP/587          | Blocked         | 1               |
| 04-15 15:43                                      | 23.195.216.135 (a23-195-216-135.deploy.static.akamaitechnologies.com) | HTTP             | Blocked         | 1               |
| 04-15 15:43                                      | 23.195.216.135 (a23-195-216-135.deploy.static.akamaitechnologies.com) | HTTP             | Blocked         | 1               |

For further reading, check out [Data leak prevention](#) in the [FortiOS 5.2 Handbook](#).

# Protecting a web server

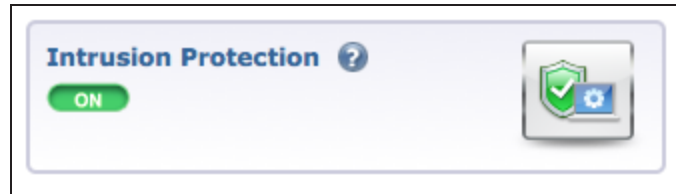


In this example, you will protect a web server using an Intrusion Prevention System (IPS) profile and a Denial of Service (DoS) policy. This will prevent a variety of different attacks from reaching the server.

A video of this recipe is available [here](#).

## 1. Enabling Intrusion Protection

Go to **System > Config > Features** and ensure that **Intrusion Protection** is turned **ON**. Apply your changes if necessary.



## 2. Configuring the default IPS profile to block common attacks

Go to **Security Profiles > Intrusion Protection** and edit the **default** profile.

In the **Pattern Based Signatures and Filters** list, highlight the default entry and select **Edit**.

| Pattern Based Signatures and Filters |        |        |         |                |  |
|--------------------------------------|--------|--------|---------|----------------|--|
| Create New                           | Edit   | Delete |         |                |  |
| Severity                             | Target | OS     | Action  | Packet Logging | Matched Signatures   |
| Medium, High, Critical               | All    | All    | Default |                | 3Com.3CDaemon.FTP.Server.Buffer.Overflow<br>3Com.Intelligent.Management.Center.Directory.Traversal<br>...<br>[Show all 4577] |

Select **Severity** to view all signatures in the database.

|  |   |   |
|--|---|---|
| <b>Severity</b> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Critical</li><li><input checked="" type="checkbox"/> High</li><li><input checked="" type="checkbox"/> Medium</li><li><input checked="" type="checkbox"/> Low</li><li><input checked="" type="checkbox"/> Information</li></ul> | <b>Target</b> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> client</li><li><input checked="" type="checkbox"/> server</li></ul> | <b>OS</b> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> BSD</li><li><input checked="" type="checkbox"/> Linux</li><li><input checked="" type="checkbox"/> MacOS</li><li><input checked="" type="checkbox"/> Other</li><li><input checked="" type="checkbox"/> Solaris</li><li><input checked="" type="checkbox"/> Windows</li></ul> |
|--|---|---|

Scroll down and set the **Action** to **Block All**.

|               |   |                                   |  |                             |                                  |
|---------------|---|-----------------------------------|--|-----------------------------|----------------------------------|
| <b>Action</b> | <input checked="" type="radio"/> Signature Defaults | <input type="radio"/> Monitor All | <input checked="" type="radio"/> Block All | <input type="radio"/> Reset | <input type="radio"/> Quarantine |
|---------------|---|-----------------------------------|--|-----------------------------|----------------------------------|



Enable all the listed **Rate Based Signatures**.

| Rate Based Signatures |  |           |                    |          |        |                          |
|-----------------------|--|-----------|--------------------|----------|--------|--------------------------|
| Enable                | Signature  | Threshold | Duration (seconds) | Track By | Action | Block Duration (minutes) |
|                       | Apache.HTTP.Server.Range.DoS                       | 30        | 1                  | Any      |        | 0                        |
|                       | Digium.Asterisk.File.Descriptor.DoS                | 20        | 1                  | Any      |        | 0                        |
|                       | Digium.Asterisk.IAX2.Call.Number.DoS               | 275       | 1                  | Any      |        | 0                        |
|                       | DotNetNuke.Padding.Oracle.Attack                   | 1000      | 5                  | Any      |        | 0                        |
|                       | FTP.Login.Brute.Force                              | 200       | 10                 | Any      |        | 0                        |
|                       | FreeBSD.TCP.Reassembly.DoS                         | 10        | 2                  | Any      |        | 0                        |
|                       | IMAP.Login.Brute.Force                             | 60        | 10                 | Any      |        | 0                        |
|                       | Lotus.Domino.Login.Brute.Force                     | 300       | 10                 | Any      |        | 0                        |
|                       | MS.Active.Directory.LDAP.Packet.Handling.DoS       | 100       | 1                  | Any      |        | 0                        |
|                       | MS.RDP.Connection.Brute.Force                      | 200       | 10                 | Any      |        | 0                        |
|                       | MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy | 35        | 1                  | Any      |        | 0                        |
|                       | MS.Windows.SMB.Server.NTLM.Authentication.Bypass   | 1000      | 1                  | Any      |        | 0                        |
|                       | MS.XML.Core.Services.Memory.Corruption             | 5         | 10                 | Any      |        | 0                        |
|                       | MySQL.Login.Brute.Force                            | 60        | 60                 | Any      |        | 0                        |
|                       | Novell.Open.Enterprise.Server.HTTPSTK.DoS          | 19        | 1                  | Any      |        | 0                        |
|                       | POP3.Login.Brute.Force                             | 200       | 10                 | Any      |        | 0                        |
|                       | SMB.Login.Brute.Force                              | 500       | 60                 | Any      |        | 0                        |
|                       | SSH.Connection.Brute.Force                         | 200       | 10                 | Any      |        | 0                        |
|                       | Telnet.Login.Brute.Force                           | 60        | 60                 | Any      |        | 0                        |
|                       | Wordpress.Login.Brute.Force                        | 1000      | 10                 | Any      |        | 0                        |

### 3. Adding the IPS sensor to the server access security policy

Go to **Policy & Objects > Policy > IPv4** and edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** under **Security Profiles** and set it to use the **default** profile.

Enabling IPS will automatically enable **SSL Inspection**. In order to inspect encrypted traffic, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).

Incoming Interface

wan1

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

internal

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Destination Interface Address

Use Dynamic IP Pool

Fixed Port

Click to add...

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

default

OFF

Application Control

default

ON

IPS

default

OFF

DLP Sensor

default

ON

SSL/SSH Inspection

deep-inspection

## 4. Creating a DoS policy

Go to **Policy & Objects > Policy > DoS** and create a new policy.


Set **Incoming Interface** to your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.


Incoming Interface

wan1


Source Address

 all

Destination Address

 all

Service

 ALL

Anomalies

| Name             | <input checked="" type="checkbox"/> Status | <input checked="" type="checkbox"/> Logging | Action | Threshold |
|------------------|--|---|--------|-----------|
| tcp_syn_flood    | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 2000      |
| tcp_port_scan    | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 1000      |
| tcp_src_session  | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| tcp_dst_session  | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| udp_flood        | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 2000      |
| udp_scan         | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 2000      |
| udp_src_session  | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| udp_dst_session  | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| icmp_flood       | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 250       |
| icmp_sweep       | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 100       |
| icmp_src_session | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 300       |
| ip_dst_session   | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| sctp_flood       | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 2000      |
| sctp_scan        | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 1000      |
| sctp_src_session | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |
| sctp_dst_session | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>         | Block  | 5000      |

ON

Enable this policy

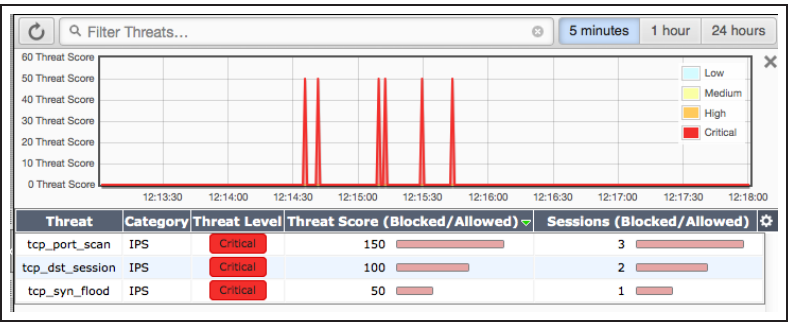
## 5. Results

Warning: DoS attacks are illegal, unless you own the server under attack. Before performing an attack, ensure that you have the correct server IP.

Launch a DoS attack on your web server's IP address.

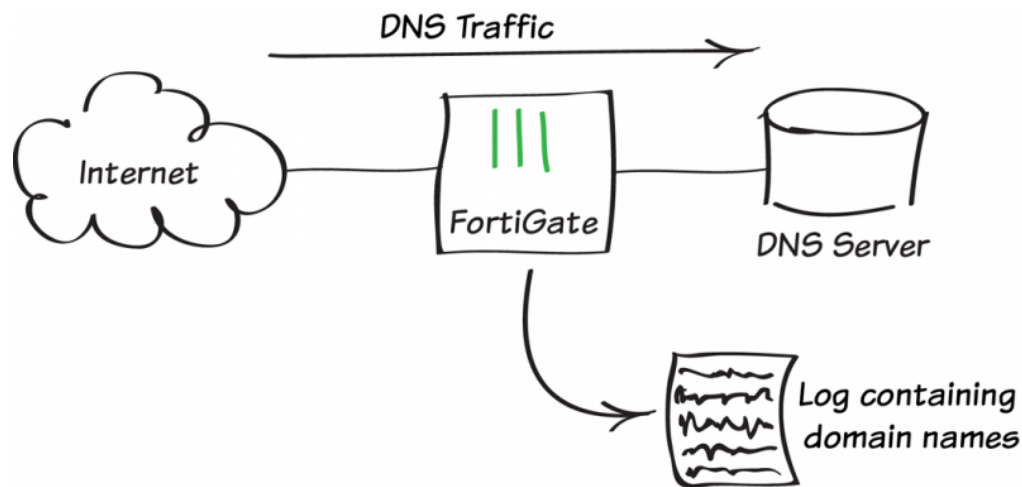
Go to **System > FortiView > Threats** and select the **5 Minutes** view.

You will see that a DoS attack has been detected and blocked.



For further reading, check out [Intrusion Protection](#) in the [FortiOS 5.2 Handbook](#).

# Logging DNS domain lookups



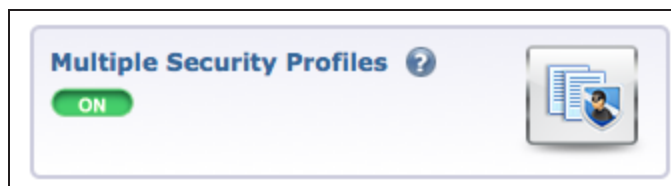
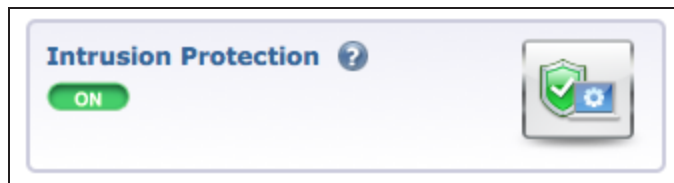
In this recipe, you will add a custom Intrusion Protection (IPS) signature to a security policy to record all domain lookups accepted by the policy. The signature records an IPS log message containing the domain name every time a DNS lookup occurs.

## 1. Enabling Intrusion Protection and multiple security profiles

Go to **System > Config > Features** and enable **Intrusion Protection**.

Select **Show More** and enable **Multiple security profiles**.

**Apply** the changes.



## 2. Creating a custom IPS signature

Go to **Security Profiles > Intrusion Protection** and select **View IPS Signatures**.

Create a new signature with this syntax. (You can copy and paste this text into the **Signature** field.)

|           |  |
|-----------|--|
| Name      | <input type="text" value="log-DNS_QUERY"/>                             |
| Signature | <input type="text" value="F-SBID( --name DOM-ALL; --protocol udp; -"/> |

```
F-SBID( --name DOM-ALL; --protocol udp; --service  
dns; --log DNS_QUERY;)
```

## 3. Adding the signature to an IPS profile

Go to **Security Profiles > Intrusion Protection** and create a new profile.

|          |  |
|----------|--|
| Name     | <input type="text" value="DNS-logging"/> |
| Comments | <input type="text" value=""/> 0/255      |

Under **Pattern Based Signatures and Filters**, select **Create New**.

Set **Sensor Type** to Specify Signatures. The new signature should appear at the top of the list. If it does not, search for the signature's name (in the example, *log-DNS\_QUERY*).

Select the signature, then select **OK**.

Sensor Type

☐ Filter Based

☒ Specify Signatures

Filter Options

☒ Basic

☐ Advanced

[\[Show Filter\]](#)

Type to search signatures

☐ Show Selected Signatures Only

| Signature  | Severity | Target         |
|--|----------|----------------|
| [Custom] log-DNS_QUERY   |          |                |
| 3Com.3CDaemon.FTP.Server.Buffer.Overflow                       | High     | server         |
| 3Com.3CDaemon.FTP.Server.Information.Disclosure                | Low      | client         |
| 3Com.Intelligent.Management.Center.Directory.Traversal         | Medium   | server         |
| 3Com.Intelligent.Management.Center.Information.Disclosure      | Medium   | server         |
| 3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS           | Medium   | server         |
| 3ivx.MPEG4.File.Processing.Buffer.Overflow                     | High     | client         |
| 7Technologies.IGSS.SCADA.System.Directory.Traversal            | Critical | server         |
| 427BB.Cookie.Based.Authentication.Bypass                       | Medium   | server         |
| 427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection           | Medium   | server         |
| ABB.MicroSCADA.Wserver.Command.Execution                       | Medium   | server         |
| ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow | Critical | server         |
| ABB.T.S.Viewer.CWGraph3D.ActiveX.Arbitrary.File.Creation       | Medium   | client         |
| ABB.S.Audio.Media.Player.LST.Buffer.Overflow                   | High     | server, client |
| ACal.Calendar.Cookie.Based.Authentication.Bypass               | High     | server         |

1

/ 320

[ Total: 4790 ]

Action

☒ Signature Defaults

☒ Monitor All

☒ Block All

☒ Reset

☒ Quarantine

☐ Packet Logging

OK

Cancel

#### 4. Adding the profile to the DNS server's security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing traffic to reach the DNS server.

Under **Security Profiles**, enable **IPS** and select the new profile.

Security Profiles

OFF

AntiVirus

OFF

Web Filter

OFF

Application Control

ON

IPS

ON

SSL/SSH Inspection

default

default

default

DNS-logging

certificate-inspection

Under **Logging Options**, enable **Log Allowed Traffic** and select **Security Events**.

Logging Options

☒ Log Allowed Traffic

☒ Security Events

☐ All Sessions

## 5. Results

Go to **Log & Report > Security Log > Intrusion Protection**.

*This log only appears when an IPS event has occurred.*

You will see that the IPS profile has detected matching traffic.

If you select an entry, you can view more information.

The domain name is shown in the **Message** field.

If you have a FortiAnalyzer, you can create a custom dataset for the DNS query by going to **Reports > Advanced > Dataset**.

| #  | Date/Time | Severity | Source          | Protocol | User | Action   | Count | Attack Name |
|----|-----------|----------|-----------------|----------|------|----------|-------|-------------|
| 1  | 07:51:31  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 2  | 07:51:32  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 3  | 07:51:32  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 4  | 07:51:31  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 5  | 07:51:32  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 6  | 07:51:31  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 7  | 07:51:31  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 8  | 07:51:32  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 9  | 07:51:32  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |
| 10 | 07:51:31  | *****    | 192.168.200.110 | udp      |      | detected |       | DOM-ALL     |

|            |  |                     |               |
|------------|--|---------------------|---------------|
| #          | 38                                     | Action              | detected      |
| Attack ID  | 4153                                   | Attack Name         | DOM-ALL       |
| Date/Time  | 07:51:29                               | Destination         | 192.168.110.9 |
| Direction  | 0                                      | Dst Port            | 53            |
| Event Type | signature                              | Incident Serial No. | 216891970     |
| Level      | *****                                  | Log ID              | 16384         |
| Message    | custom: DOM-ALL, dns_query=trello.com; |                     |               |
| Protocol   | udp                                    | Profile Name        | DNS-logging   |
|            |  | Protocol Number     | 17            |

Name

DNS-Query

Log Type

Attack

Query

```
select msg, sum(totalnum) as totalnum from
###(select srcip, msg, count(*) as totalnum from
$log where $filter-exclude-var group by srcip,
msg order by totalnum desc)### t where $filter-
var-only and msg is not null group by msg order
by totalnum desc
```

This dataset can then be used in a custom report.

FORTINET

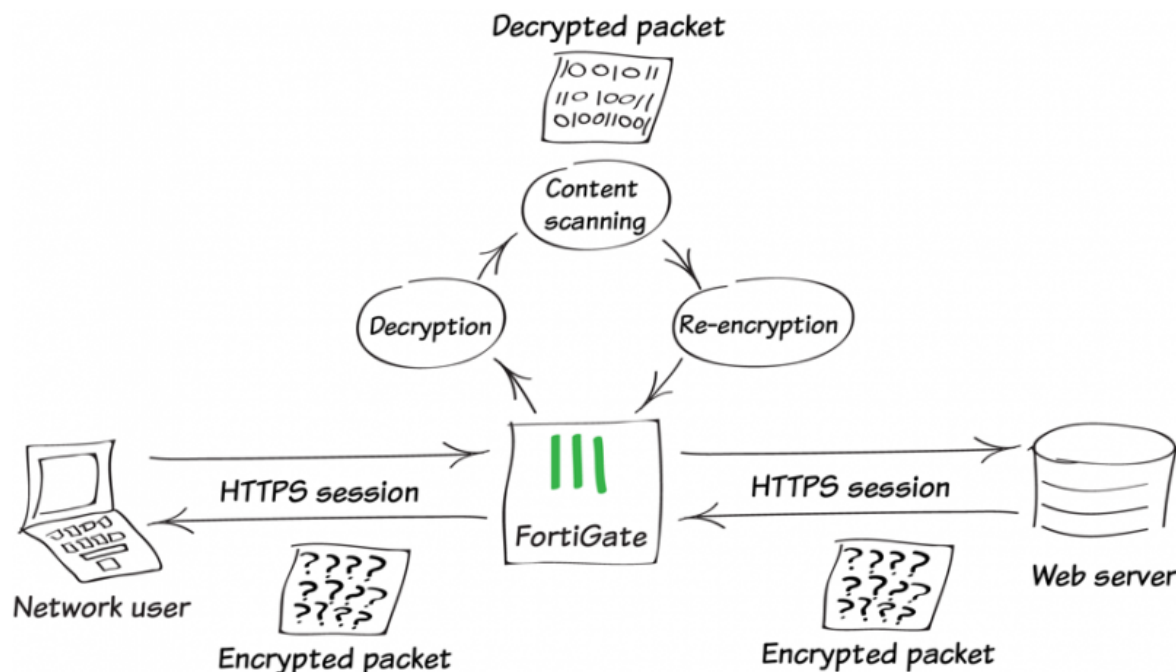
TOP 10 requested DNS Domains

| #  | Message  | totalnum | % of Total |
|----|--|----------|------------|
| 1  | custom: DNS-A-Request, dns_query=init-p01st.push.apple.com;        | 57       | 3.68       |
| 2  | custom: DNS-A-Request, dns_query=init-s01st.push.apple.com;        | 49       | 3.17       |
| 3  | custom: DNS-A-Request, dns_query=www.google.com;                   | 49       | 3.17       |
| 4  | custom: DNS-A-Request, dns_query=www.apple.com;                    | 44       | 2.84       |
| 5  | custom: DNS-A-Request, dns_query=local;                            | 40       | 2.58       |
| 6  | custom: DNS-A-Request, dns_query=apple.com;                        | 38       | 2.45       |
| 7  | custom: DNS-A-Request, dns_query=p07-btmdns.icloud.com;            | 34       | 2.20       |
| 8  | custom: DNS-A-Request, dns_query=apple-mobile.query.yahooapis.com; | 31       | 2.00       |
| 9  | custom: DNS-A-Request, dns_query=dell.com;                         | 30       | 1.94       |
| 10 | custom: DNS-A-Request, dns_query=api.bing.com;                     | 26       | 1.68       |
| 11 | Others   | 1150     | 74.29      |
| 12 | Total  | 1548     | 100.00     |

For further reading, check out [DNS Service](#) in the [FortiOS 5.2 Handbook](#).



# Why you should use SSL inspection



Most of us are familiar with the benefits of Hypertext Transfer Protocol Secure (HTTPS) and how it protects most commerce activities on the Internet. HTTPS applies Secure Sockets Layer (SSL) encryption to secure web traffic from prying eyes. The benefits are obvious; the risks, however are not as obvious, though they do exist.

One major risk is that encrypted traffic could be used in attacks that get around your normal defences. For example, you could download a file containing a virus during an e-commerce session. Because the session is encrypted your normal defences would miss it.

In another example, you could receive a phishing email that contains a seemingly harmless downloader file. When launched, the downloader could create an encrypted HTTPS session to a command and control (C&C) server that downloads malware onto your computer. Because the session containing the malware is encrypted, your antivirus protection can't see and block the threat.

To protect your network from these threats, SSL inspection is the key that your FortiGate can use to unlock encrypted sessions, see into encrypted packets, find threats, and block them. SSL inspection not only protects you from attacks that use HTTPS, but also from other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

## Full SSL inspection

To make sure that all SSL encrypted content is inspected, you must use full SSL inspection, which is also known as deep inspection. When full SSL inspection is used, the FortiGate impersonates the recipient of the originating SSL session, decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender and sends the content to the sender.

When the FortiGate re-encrypts the content it uses a certificate stored on the FortiGate. The client must trust this certificate to avoid certificate errors. Whether or not this trust exists depends on the client, which can be the computer's OS, a browser or some other application, which will likely maintain its own certificate repository. For more information about this, see the recipe [Preventing certificate warnings](#).

There are two deployment methods for full SSL inspection:

### Multiple Clients Connecting to Multiple Servers:

- Uses a CA certificate (which can be upload by going to **System > Certificates > CA Certificates**).
- Typically applied to outbound policies where destination are unknown (i.e. normal web traffic).
- Address and web category whitelists can be configured to bypass SSL inspection.

### Protecting SSL Server

- Uses a server certificate (which can be upload by going to **System > Certificates > CA Certificates**) to protect a single server.
- Typically used on inbound policies to protect servers available externally through Virtual IPs
- Since this is typically deployed "outside-in" (clients on the Internet accessing server(s) on the internal side of the FortiGate), server certificates using the public FQDN of the server are often purchased from a commercial Certificate Authority and uploaded to the FortiGate. This avoids client applications generating SSL certificate errors due to certificate mismatch.

More detail is available in the [FortiOS 5.2 Handbook](#). Also, check the Fortinet Knowledge Base for these technical notes:

- [How to Enable SSL inspection from the CLI and Apply it to a Policy](#)
- [How to block web-based chat on Gmail webmail using App Sensor + SSL inspection](#)

## SSL certificate inspection

FortiGates also support a second type of SSL inspection, called SSL certificate inspection. When certificate inspection is used, the FortiGate only inspects the header information of the packets.

Certificate inspection is used to verify the identity of web servers and can be used to make sure that HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. However, since only the packet is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

## Troubleshooting

The most common problem with SSL inspection is users receiving SSL errors when the CA certificate is not trusted. This is because by default the FortiGate uses a certificate that is not trusted by the client. There are two ways to fix this:

- All users must import the FortiGate's default certificate into their client applications as a trusted certificate.
- Configure the FortiGate to use a certificate that is already trusted by your clients. For example, a certification signed by a CA that your clients already trust.

The first method can be more labor intensive because you have to distribute a certification to all clients. This can also be an ongoing problem as new clients are added to your network. The second method is usually less work but may require paying for a CA. Both of these methods are covered in the recipe [Preventing Certificate Warnings](#).

If you choose to install the cert on clients, this can be easier in a Microsoft Active Directory domain by using Group Policy Objects to install the certificate on domain members. Check that the Group Policy has propagated to all computers by opening Internet Explorer on a workstation PC, opening **Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities**, and ensuring that the FortiGate's certificate is present.

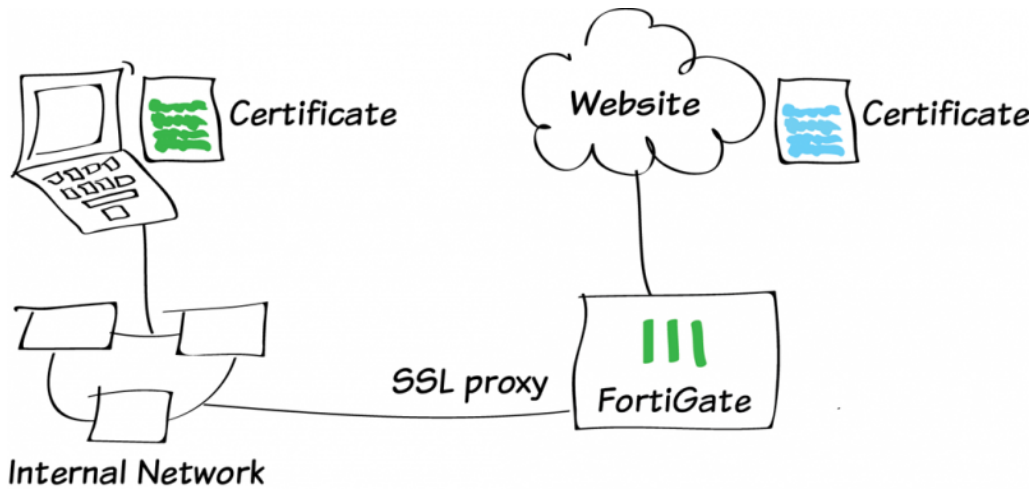
For corporate-owned mobile devices, MDM solutions like AirWatch, MobileIron, or Fiberlink, use Simple Certificate Enrollment Protocol (SCEP) to ease certificate enrollment.

## Best practices

Because all traffic needs to be decrypted, inspected, and re-encrypted, using SSL inspection can reduce overall performance of your FortiGate. To make sure you aren't using too many resources for SSL inspection, do the following:

- **Know your traffic** – Know how much traffic is expected and what percent of the traffic is encrypted. You can also limit the number of policies that allow encrypted traffic.
- **Be selective** – Use white lists or trim your policy to apply SSL inspection only where it is needed.
- **Use hardware acceleration** - FortiGate models with either the CP6 or CPU processor have an SSL/TLS protocol processor for SSL content scanning and SSL acceleration. For more information about this, see the [Hardware Acceleration handbook](#).
- **Test real-world SSL inspection performance yourself** - Use the flexibility of FortiGate's security policy to gradually deploy SSL inspection, rather than enabling it all at once.

# Preventing certificate warnings



This example illustrates how to prevent your users from getting a security certificate warning when you have enabled full SSL inspection (also called deep inspection).

Instead of having users select **Continue** when they receive a warning, a bad habit to encourage, you can use the examples below to prevent certificate warnings from appearing: [Using the default FortiGate certificate](#) or [Using a self-signed certificate](#).

For more information about SSL inspection, see [Why you should use SSL inspection](#).

# Using the default FortiGate certificate

All FortiGates have a default certificate that is used for SSL deep inspection. This certificate is also used in the default **deep-inspection** profile.

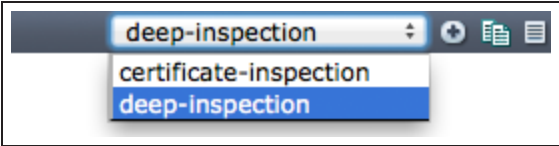
To prevent your users from seeing certificate warnings you can distribute this certificate to your user's devices.

A video of this example can be found [here](#).

## 1. Viewing the deep-inspection SSL profile

Go to **Policy & Objects > SSL/SSH Inspection**. In the upper-right hand drop down menu, select **deep-inspection**.

*The deep-inspection profile will apply SSL inspection to the content of all encrypted traffic.*



In this policy, the web categories **Health and Wellness**, **Personal Privacy**, and **Finance and Banking** are excluded from SSL inspection by default. Applications that require unique certificates, such as iTunes and Dropbox, have also been excluded.

Name

deep-inspection

Comments

Deep inspection.16/255

SSL Inspection Options

Enable SSL Inspection of

Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

CA Certificate

Fortinet\_CA\_SSLProxy

Inspection Method

SSL Certificate Inspection

Full SSL Inspection

Inspect All Ports

ON

HTTPS443

ON

SMTPS465

ON

POP3S995

ON

IMAPS993

ON

FTPS990

Exempt from SSL Inspection

Web Categories

Health and WellnessX+

Personal PrivacyX

Finance and BankingX

Addresses

androidX+

appleX

appstore.comX

citrixonlineX

dropbox.comX

GotomeetingX

icloudX

itunesX

skypeX

swscan.apple.comX

update.microsoft.comX

## 2. Enabling certificate configuration in the web-based manager

Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply** the changes.

Certificates?

ON

Changes:

No changes

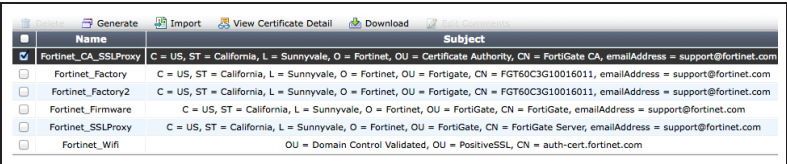
Apply

Reset

### 3. Downloading the Fortinet\_CA\_SSLProxy certificate

Go to **System > Certificates > Local Certificates** to download the **Fortinet\_CA\_SSLProxy** certificate.

Make the CA certificate file available to your users by checkmarking the box next to the certificate name.



|                                     | Name                 | Subject  |
|-------------------------------------|----------------------|--|
| <input checked="" type="checkbox"/> | Fortinet_CA_SSLProxy | C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com |
| <input type="checkbox"/>            | Fortinet_Factory     | C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FGT60C3G10016011, emailAddress = support@fortinet.com         |
| <input type="checkbox"/>            | Fortinet_Factory2    | C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = FGT60C3G10016011, emailAddress = support@fortinet.com         |
| <input type="checkbox"/>            | Fortinet_Firmware    | C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FortiGate, emailAddress = support@fortinet.com                |
| <input type="checkbox"/>            | Fortinet_SSLProxy    | C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FortiGate Server, emailAddress = support@fortinet.com         |
| <input type="checkbox"/>            | Fortinet_Wifi        | OU = Domain Control Validated, OU = PositiveSSL, CN = auth-cert.fortinet.com   |

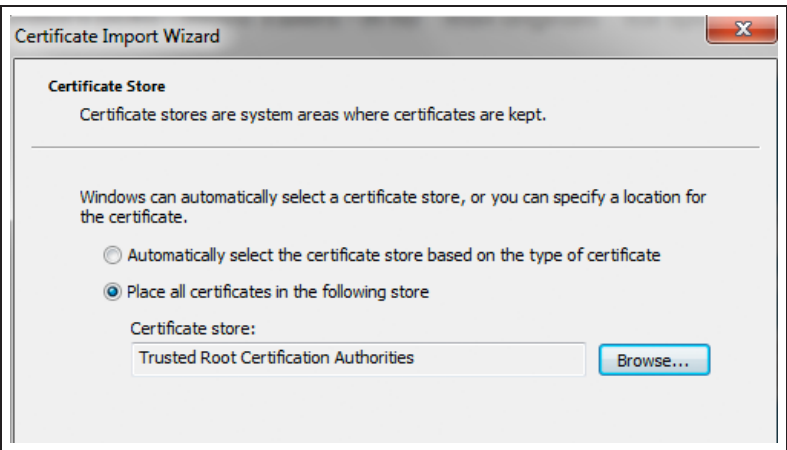
### 4. Importing the CA certificate into the web browser

For Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

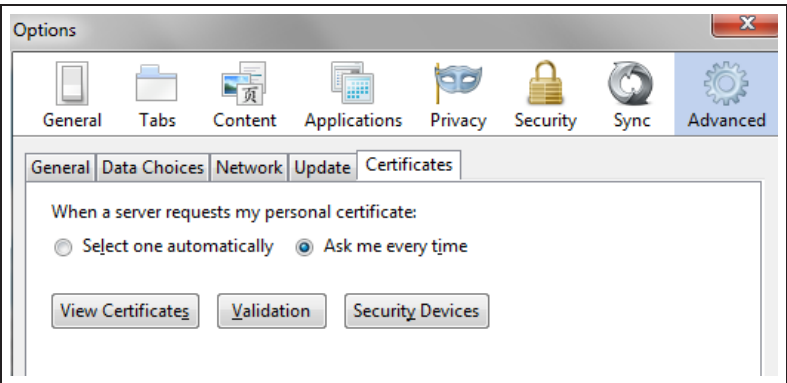
Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.

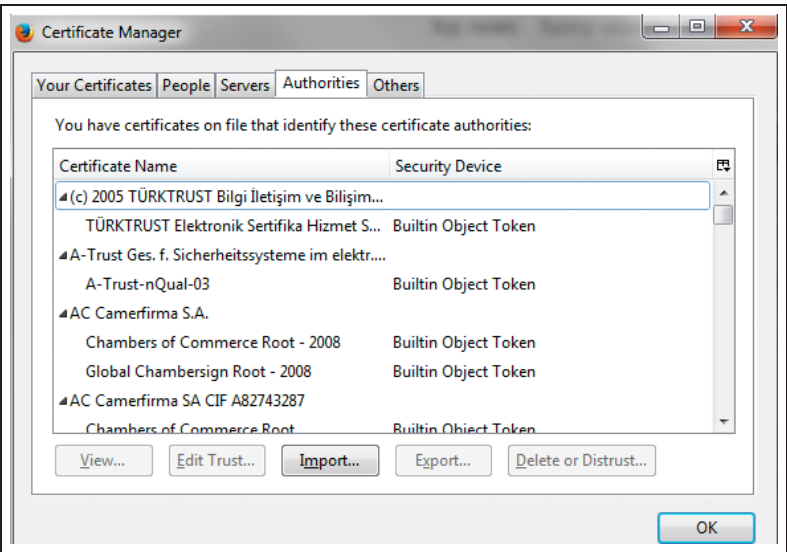


For Firefox:

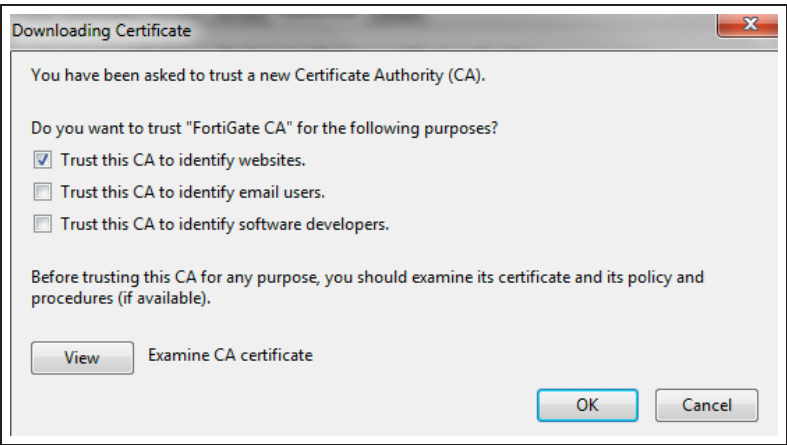
Depending on the platform, go to **Menu > Options** or **Preferences > Advanced** and find the **Certificates** tab.



Click **View Certificates**, specifically the **Authorities** certificate list.



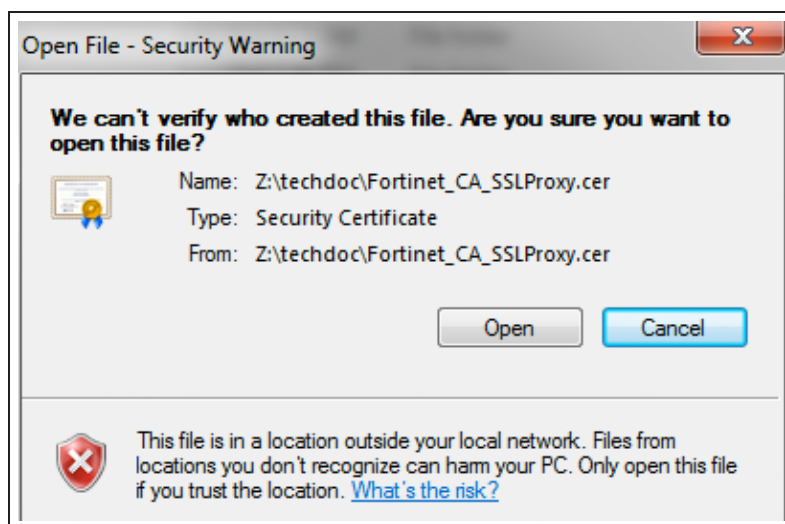
Click **Import** and select the **Fortinet\_CA\_SSLProxy** certificate file.





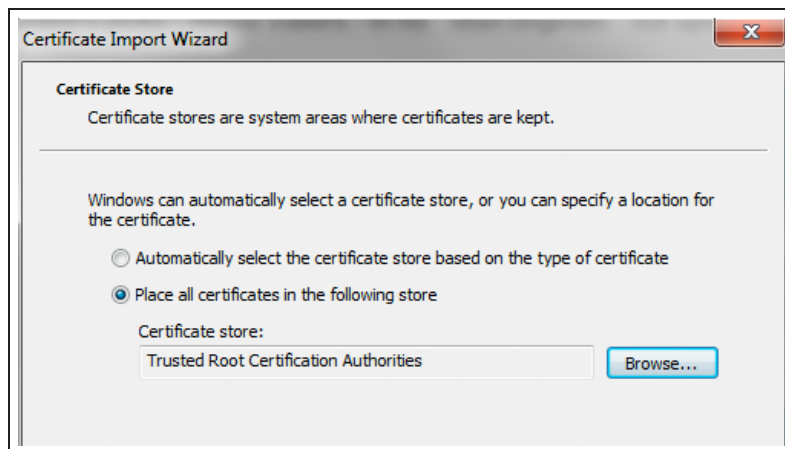
For Google Chrome and Safari:

Locate and open the downloaded **Fortinet\_CA\_SSLProxy** certificate file. Choose **Open** and click **Install Certificate**. The Import Wizard appears.



Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.



## 5. Results

Before installing the FortiGate SSL CA certificate, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.

After you install the FortiGate SSL CA certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.

iTunes will now be able to run without a certificate error.



For further reading, check out [SSL/SSH Inspection](#) in the [FortiOS 5.2 Handbook](#).

# Using a self-signed certificate

In this method, a self-signed certificate is created using OpenSSL. This certificate will then be installed on the FortiGate for use with SSL inspection.

In this recipe, OpenSSL for Windows version 0.9.8h-1 is used.

A video of this example can be found [here](#).

## 1. Creating a certificate with OpenSSL

If necessary, download and install Open SSL. Make sure that the file *openssl.cnf* is located in the *BIN* folder for OpenSSL.

Using Command Prompt (CMD), navigate to the BIN folder (in the example, the command is `cd c:\OpenSSL\openssl-0.9.8h-1\bin\bin`).

Generate an RSA key with the following command:

```
OpenSSL genrsa -aes256 -out fgcprivkey.pem 2048 -config openssl.cnf
```

This RSA key uses AES 256 encryption and a 2058-bit key.

When prompted, enter a pass phrase for encrypting the private key.

Use the following command to launch OpenSSL, submit a new certificate request, and sign the request:

```
openssl req - new -x509 -days 3650 -extensions v3_ca -key fgcprivkey.pem -out fgcacert.pem - config openssl.cnf
```

The result is a standard x509 binary certificate that is valid for 3,650 days (approx. 10 years)

When prompted, re-enter the pass phrase for encryption, then enter the details required for the certificate request, such as location and organization name.

Two new files have been created: a public certificate (*fgcacert.pem*) and a private key (in the example, *fgcprivkey.pem*).

## 2. Enabling certificate configuration in the web-based manager

Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply** the changes.

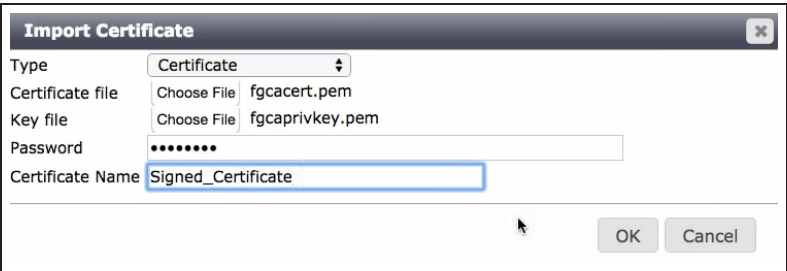


## 3. Importing the self-signed certificate



Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate Unit.

Go to **System > Certificates** and select **Import**.

From the **Type** drop down menu select **Certificate**. Select **Choose File** to set your **Certificate file** to your public certificate and **Key file** to your private key. Enter the **Password** used when generating the certificate. If desired, you may also set a new **Certificate Name**.



The certificate now appears on the **Local Certificates** list.

| Name   | Subject   |
|--|---|
| Local CA Certificates (2)  |   |
|  Fortinet_CA_SSLProxy | C = US, CN = FortiGate CA, L = Sunnyvale,<br>O = Fortinet, ST = California,<br>emailAddress = support@fortinet.com,<br>OU = Certificate Authority |
|  Signed_Certificate   | C = CA, CN = www.fortinet.com, L = Ottawa,<br>O = Fortinet, ST = Ontario,<br>emailAddress = krobinsn@fortinet.com,<br>OU = Docs,Certificates, VPN |

## 4. Edit the SSL inspection profile

To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**. Edit

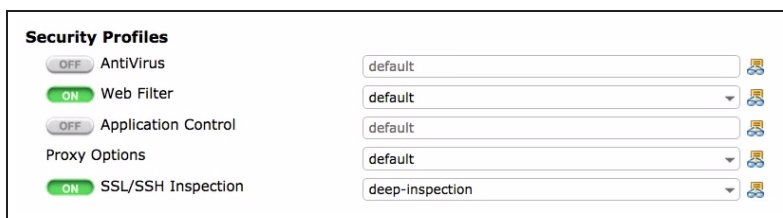
the **deep-inspection** profile.

In the **CA Certificate** drop down menu, select the certificate you imported.

## 5. Editing your Internet policy to use full SSL inspection

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic. Under **Security Profiles**, set **SSL Inspection** to **deep-inspection**.

For testing purposes, make sure **Web Filter** is set to **default**.

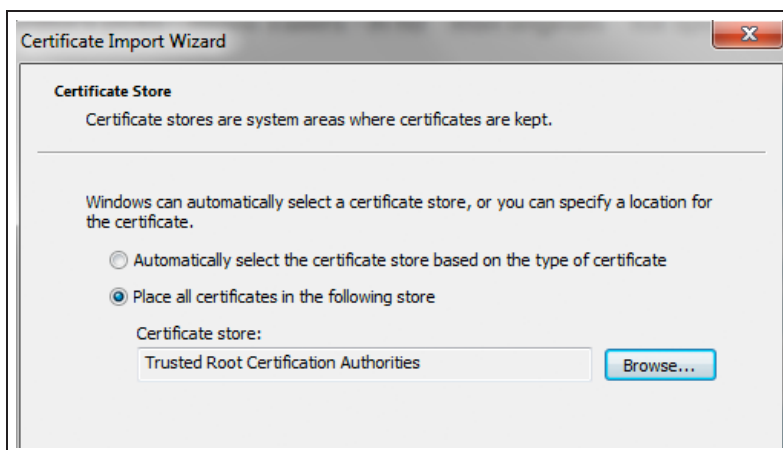


## 6. Importing the CA certificate into the web browser

Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates**.

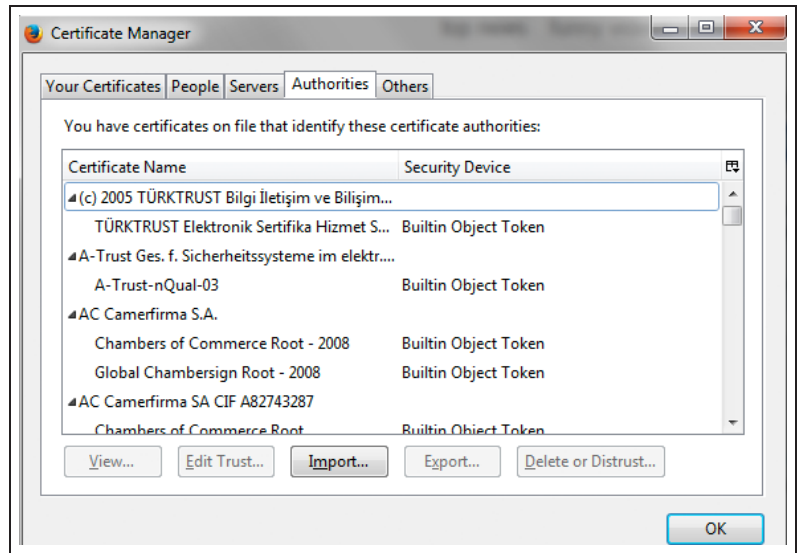
Go to **Personal** and import the certificate.



For Firefox:

Depending on the version, go to **Menu > Options** or **Preferences > Advanced** and find the **Certificates** tab.

Select **View Certificates**, then select the **Servers** list. **Import** the certificate file.

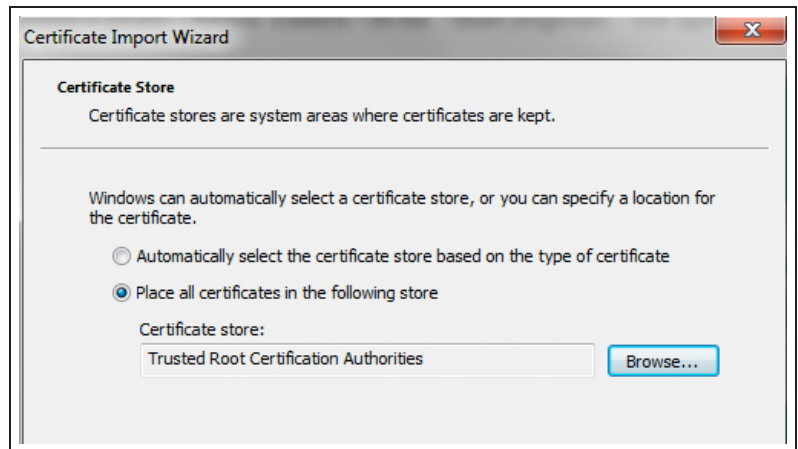


## Chrome and Safari:

If you are using Chrome or Safari, you must install the certificate for the OS, rather than directly in the browser.

If you are using Windows, open the certificate file and select **Install Certificate**. The Import Wizard appears.

Import the certificate using the Import Wizard. Import the certificate into the **Trusted Root Certification Authorities** store.



If you are using Mac OS X, open the certificate file. **Keychain Access** opens.

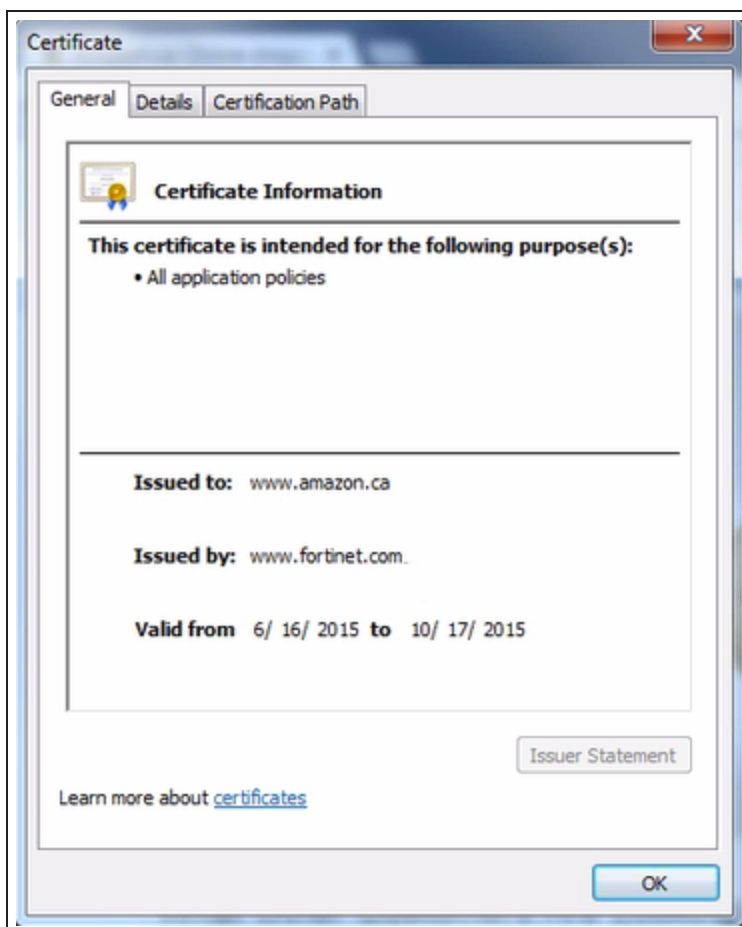
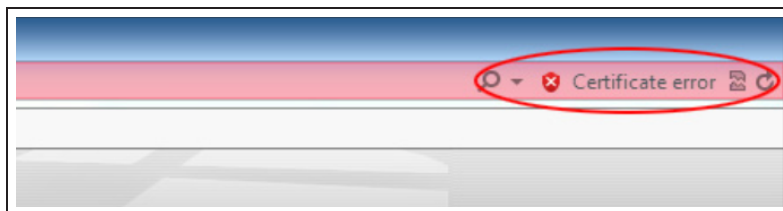
Double-click the certificate. Expand **Trust** and select **Always Trust**.

## 7. Results

Before installing the self-certificate and using it for SSL inspection, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.

After you install the self-signed certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.

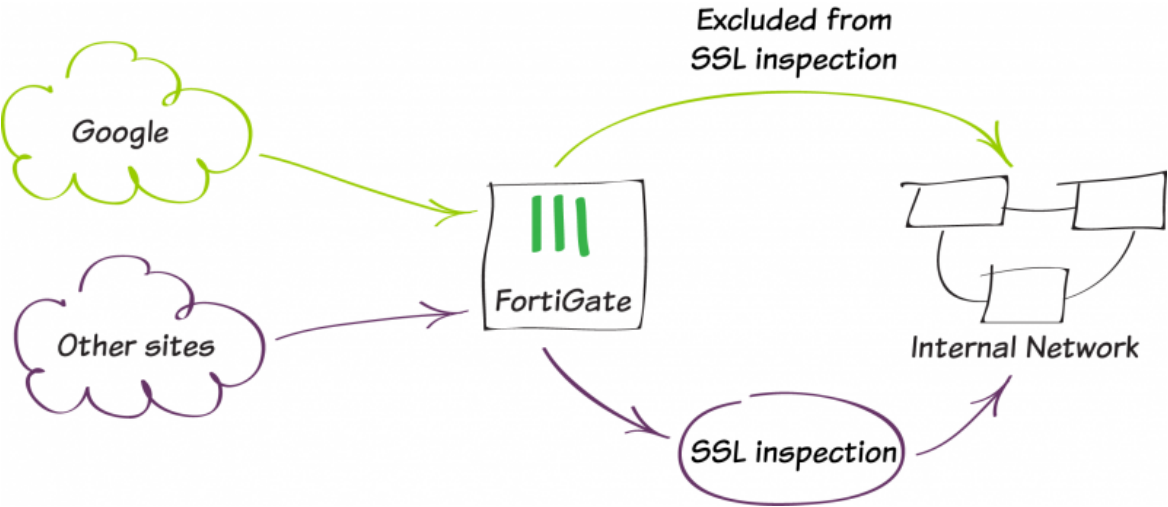
If you view the website's certificate information, the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.



For further reading, check out [SSL/SSH Inspection](#) in the [FortiOS 5.2 Handbook](#).



# Exempting Google from SSL inspection



In this recipe, you will exempt Google Canada websites from deep SSL inspection. Exempting these websites allows the Chrome browser to access them without errors.

You should use caution when exempting websites. In general, it is recommended that you only exempt website that you know you can trust. Another reason for doing this is to exempt websites that do not function properly when subjected to SSL inspection, such as a site (or application) that uses certificate/public key pinning.

In this example, google.ca is exempted from SSL inspection. If necessary, substitute your local Google search domain.

# 1. Using the deep-inspection profile

Go to **Policy & Objects > Policy > SSL/SSH Inspection** and view the **deep-inspection** profile.

By default, this profile includes a number of web categories and addresses that are listed under **Exempt from SSL Inspection**. Currently, google.ca is not included.


| Exempt from SSL Inspection |   |
|----------------------------|---|
| Web Categories             | <div>Health and Wellness X +</div> <div>Personal Privacy X</div> <div>Finance and Banking X</div>   |
| Addresses                  | <div>*.live.com X +</div> <div>adobe X</div> <div>Adobe Login X</div> <div>android X</div> <div>apple X</div> <div>appstore X</div> <div>auth.gfx.ms X</div> <div>autoupdate.opera.com X</div> <div>citrix X</div> <div>dropbox.com X</div> <div>ease X</div> <div>firefox update server X</div> <div>fortinet X</div> <div>google-drive X</div> <div>google-play X</div> <div>google-play2 X</div> <div>google-play3 X</div> <div>googleapis.com X</div> <div>Gotomeeting X</div> <div>icloud X</div> <div>itunes X</div> <div>microsoft X</div> <div>skype X</div> <div>softwareupdate.vmware.com X</div> <div>swscan.apple.com X</div> <div>update.microsoft.com X</div> <div>verisign X</div> <div>Windows update 2 X</div> |

Go to **Policy & Objects > Policy > IPv4** and make sure the policy allowing connections from the internal network to the Internet uses the **deep-inspection** profile for **SSL Inspection**. For SSL inspection to be applied to traffic, make sure both **Web Filter** and **Application Control** are turned on in the policy.

| Seq.#              | Source | Destination | Schedule | Service | Action | NAT | AV     | Web Filter  | Application Control | SSL Inspection  |
|--------------------|--------|-------------|----------|---------|--------|-----|--------|-------------|---------------------|-----------------|
| lan - wan1 (1 - 1) |        |             |          |         |        |     |        |             |                     |                 |
| 1                  | all    | all         | always   | ALL     | ACCEPT |     | Enable | Web default | APP default         | deep-inspection |

Using Google Chrome, browse to google.ca. An error appears that you cannot bypass.

This occurs because Chrome uses certificate pinning (also called SSL pinning or public key pinning). This allows Chrome to determine that, because full SSL inspection is being used, the certificate from the website does not match one belonging to Google (instead it is the certificate that the SSL inspection profile is using for SSL inspection). Because of this, Chrome believes that a "man in the middle" attack is occurring and blocks you from the compromised website. For more information about why this occurs, see [Why you should use SSL inspection](#).



### Your connection is not private

Attackers might be trying to steal your information from **www.google.ca** (for example, passwords, messages, or credit cards). NET::ERR\_CERT\_AUTHORITY\_INVALID

☐ Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Hide advanced](#)

Reload

www.google.ca normally uses encryption to protect your information. When Chrome tried to connect to www.google.ca this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be www.google.ca, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit www.google.ca right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

## 2. Creating a fully qualified domain name (FQDN) address for google.ca

Go to **Policy & Objects > Objects > Addresses** and create a new address.

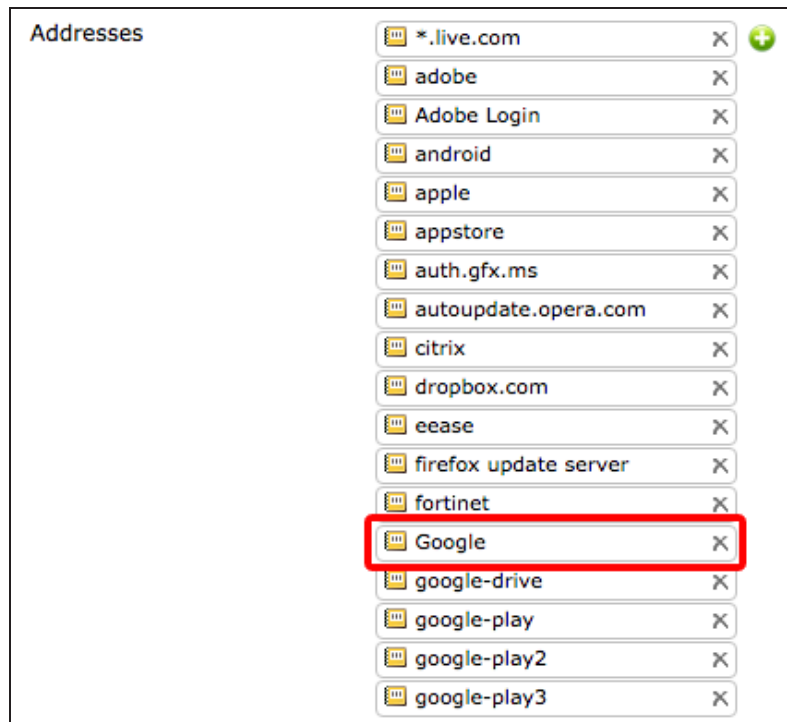
Set **Type** to **FQDN** and set **FQDN** to the URL used by Google in your region (in the example, *\*.google.ca*).

|                      |  |
|----------------------|--|
| Name                 | <input type="text" value="Google"/>      |
| Type                 | <input type="text" value="FQDN"/>        |
| FQDN                 | <input type="text" value="*.google.ca"/> |
| Interface            | <input type="text" value="any"/>         |
| Show in Address List | <input checked="" type="checkbox"/>      |
| Comments             | <div><input type="text"/></div> 0/255    |

### 3. Exempting google.ca from full SSL inspection

Go to **Policy & Objects > Policy > SSL/SSH Inspection** and edit the **deep-inspection** profile.

Add the FQDN for Google to the list of exempt **Addresses**.



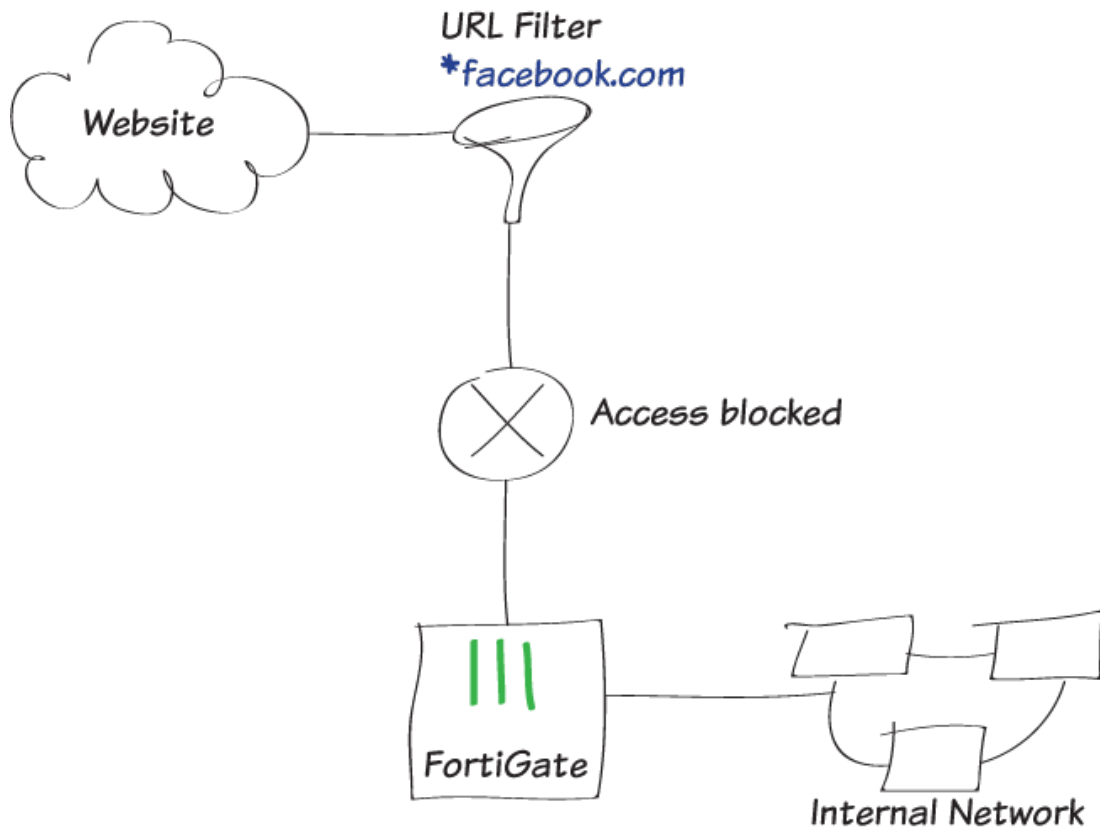
## 4. Results

Using Chrome, browse to google.ca. The site loads properly.



For further reading, check out **SSL/SSH Inspection** in the **FortiOS 5.2 Handbook**.

# Blocking Facebook



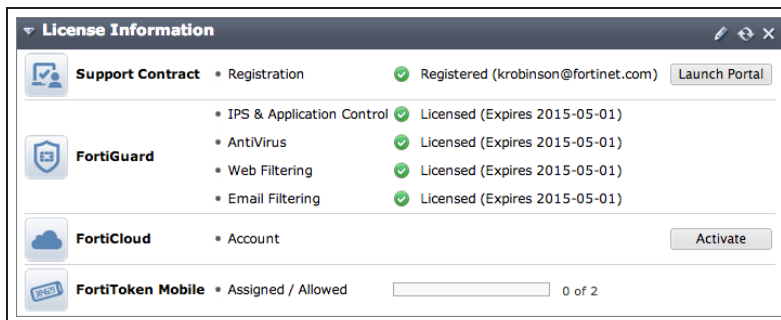
In this example, you will learn how to configure a FortiGate to prevent access to a specific social networking website, including its subdomains, by means of a static URL filter.

When you allow access to a particular type of content, such as the FortiGuard Social Networking category, there may still be certain websites in that category that you wish to prohibit. And by using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

A video of this recipe is available [here](#).

## 1. Verifying FortiGuard Services subscription

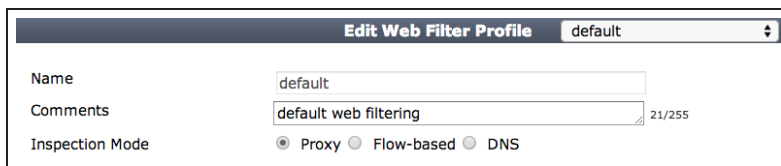
Go to **System > Dashboard > Status**. In the **License Information** widget, verify that you have an active subscription to FortiGuard Web Filtering. If you have a subscription, the service will have a green checkmark beside it.



## 2. Editing the Web Filter profile

Go to **Security Profiles > Web Filter** and edit the default Web Filter profile.

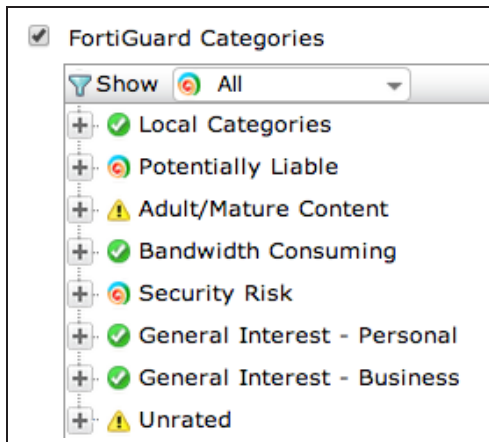
Set **Inspection Mode** to **Proxy**.



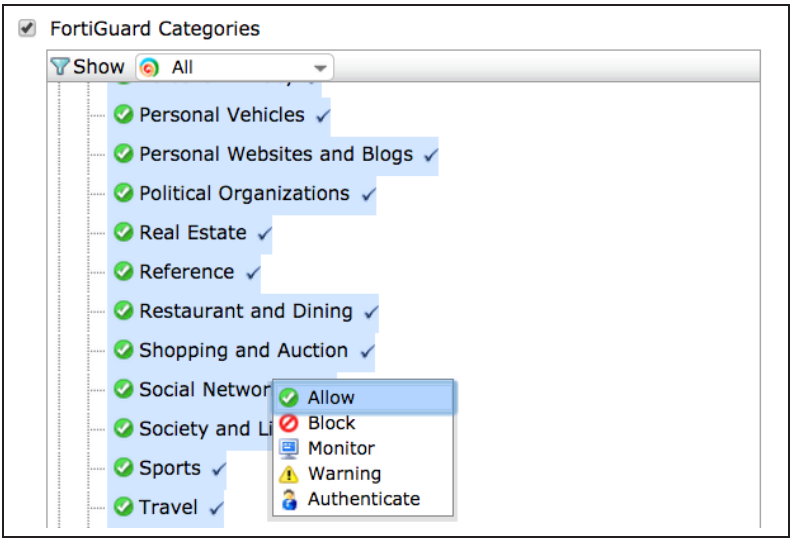
Enable the FortiGuard Categories that allow, block, monitor, warn or authenticate depending on the type of content.

*Learn more about FortiGuard Categories at the FortiGuard Center web filtering rating page:*

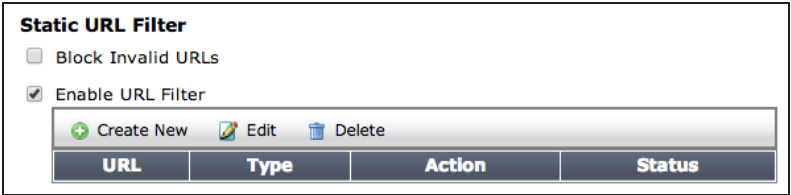
[www.fortiguards.com/static/webfiltering.html](http://www.fortiguards.com/static/webfiltering.html)



Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.

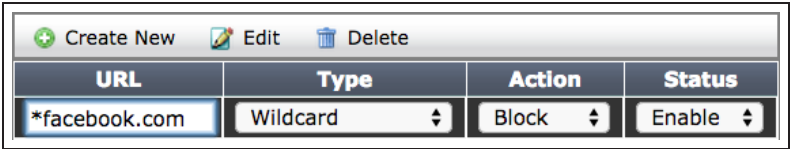


To prohibit visiting one particular social networking site in that category, go to **Static URL filter**, select **Enable URL Filter**, and then click **Create New**.



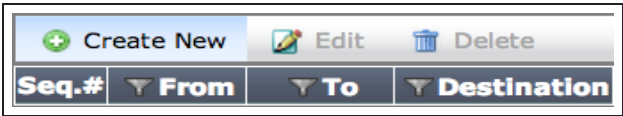
For your new web filter, enter the URL of the website you are attempting to block. If you want to block all of the subdomains for that website, omit the protocol in the URL and enter an asterisk (\*). For this example, enter: *\*facebook.com*

Set **Type** to **Wildcard**, set **Action** to **block**, and set **Status** to **Enable**.



### 3. Creating a security policy

Go to **Policy & Objects > Policy > IPv4**, and click **Create New**.





Set the **Incoming Interface** to allow packets from your internal network and set the **Outgoing Interface** to proceed to the Internet-facing interface (typically wan1).

Enable NAT.

Incoming Interface

lan

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

+

Destination Address

all

+

Schedule

always

Service

ALL

+

Action

ACCEPT

Firewall / Network Options

ON NAT

Under **Security Profiles**, enable **Web Filter** and select the **default** web filter.

Security Profiles

OFF AntiVirus

default

ON Web Filter

default

This automatically enables **SSL/SSH Inspection**. Select **certificate-inspection** from the dropdown menu.

This profile allows the FortiGate to inspect and apply web filtering to HTTPS traffic.

Proxy Options

default

ON SSL/SSH Inspection

certificate-inspection

After you have created your new policy, ensure that it is at the top of the policy list. To move your policy up or down, click and drag the far left column of the policy.

Create New Edit Delete

Section View Global View

Search

| Seq.#              | Source | Destination | ID | Schedule | Service | AV         |
|--------------------|--------|-------------|----|----------|---------|------------|
| lan - wan1 (1 - 2) |        |             |    |          |         |            |
| 1                  | all    | all         | 2  | always   | ALL     | None       |
| 2                  | all    | all         | 1  | always   | ALL     | AV default |
| Implicit (3 - 3)   |        |             |    |          |         |            |

## 4. Results

Visit the following sites to verify that your web filter is blocking websites ending in facebook.com:

- [facebook.com](https://facebook.com)
- [attachments.facebook.com](https://attachments.facebook.com)
- [camdencc.facebook.com](https://camdencc.facebook.com)
- [mariancollege.facebook.com](https://mariancollege.facebook.com)

A FortiGuard **Web Page Blocked!** page should appear.



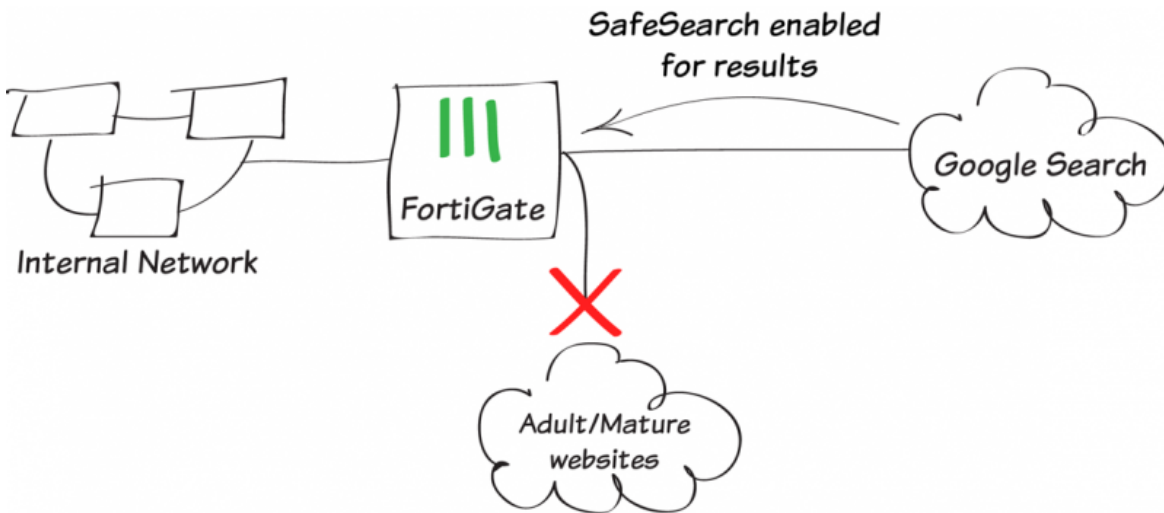
Visit <https://www.facebook.com> to verify that HTTPS protocol is blocked.

A **Web Page Blocked!** page should appear.



For further reading, check out [Static URL Filter](#) in the [FortiOS 5.2 Handbook](#).

# Blocking adult/mature content with Google SafeSearch



In this recipe, you will use FortiGate web filtering to ensure that SafeSearch is applied to all Google search results. You will also block access to websites in the adult/mature content FortiGuard category for all network users.

This recipe requires an active FortiGuard web filtering licence.

A video of this recipe is available [here](#).

## 1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.



## 2. Blocking the Adult/Mature Content category and enabling Safe Search

Go to **Security Profiles > Web Filter** and edit the default profile. Enable **FortiGuard Categories**.

Select the **Adult/Mature Content** category and set it to **Block**.

Under **Search Engines**, select **Enable Safe Search** and **Search Engine Safe Search - Google, Yahoo!, Bing, Yandex**.

### 3. Adding web filtering to your Internet access policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, enable **Web Filter** and set it to use the **default** profile.

|   |                                     |
|---|-------------------------------------|
| Incoming Interface  | internal                            |
| Source Address  | all                                 |
| Source User(s)  | Click to add...                     |
| Source Device Type  | Click to add...                     |
| Outgoing Interface  | wan1                                |
| Destination Address   | all                                 |
| Schedule  | always                              |
| Service   | ALL                                 |
| Action  | ACCEPT                              |
| <b>Firewall / Network Options</b>                               |                                     |
| <input checked="" type="checkbox"/> NAT                         |                                     |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port |
| <input type="radio"/> Use Dynamic IP Pool                       | Click to add...                     |
| <input type="radio"/> Use Central NAT Table                     |                                     |
| <b>Security Profiles</b>  |                                     |
| <input type="checkbox"/> Antivirus                              | default                             |
| <input checked="" type="checkbox"/> Web Filter                  | default                             |

### 4. Enforcing Google SafeSearch for all traffic

Because Google search often uses the HTTPS protocol, web filtering alone may not be able to block all adult/mature content. There are two methods that can be used to enforce Google SafeSearch for all traffic: using full SSL inspection so that encrypted traffic is fully inspected (which can cause certificate errors), or changing the DNS records to force search traffic to use [forcesafesearch.google.com](https://forcesafesearch.google.com).

#### Method 1: Using full SSL inspection

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **SSL/SSH Inspection** to use the **deep-inspection** profile. Using the **deep-inspection** profile may cause certificate errors. For information about

|  |                 |
|--|-----------------|
| <b>Security Profiles</b>                           |                 |
| <input type="checkbox"/> Antivirus                 | default         |
| <input checked="" type="checkbox"/> Web Filter     | default         |
| <input type="checkbox"/> Application Control       | default         |
| <input type="checkbox"/> IPS                       | default         |
| Proxy Options                                      | default         |
| <input checked="" type="checkbox"/> SSL Inspection | deep-inspection |

avoiding this, see [Preventing certificate warnings](#).

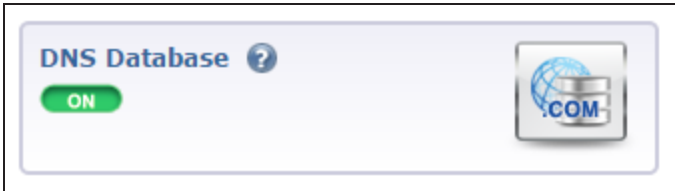
## Method 2: Changing the DNS records for www.google.com

If you wish to force Google SafeSearch for your entire network, you can set the DNS entry for `www.google.com` (and another other Google search domains, such as `www.google.[glossary_exclude]ca[/glossary_exclude]`) to be a Canonical Name (CNAME) for `forcesafesearch.google.com`. This will force all search traffic to use `forcesafesearch.google.com`.

The method for changing the DNS records using your FortiGate varies, depending on whether your FortiGate is the network's DNS server, or if an external server is used.

### FortiGate is the network's DNS server

Go to **System > Config > Features** and select **Show More**. Make sure that **DNS Database** is **ON**. If necessary, **Apply** your changes.



Go to **System > Dashboard > Status** and enter the following command into the **CLI Console** using your **internal** interface:

```
config system dns-server
edit internal
set mode recursive
end
```

Go to **System > Network > DNS Servers**. The new server is listed under **DNS Service on Interface**.

| DNS Service on Interface   |           |           |
|--|-----------|-----------|
| <a href="#">Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> |           |           |
|  | Interface | Mode      |
| <input type="checkbox"/>   | internal  | Recursive |

Under **DNS Database**, select **Create New**.

Set **DNS Zone** as *Google*, **Domain Name** to *google.com*, and disable **Authoritative**.

|                            |  |
|----------------------------|--|
| Type                       | <input checked="" type="radio"/> Master <input type="radio"/> Slave  |
| View                       | <input type="radio"/> Public <input checked="" type="radio"/> Shadow |
| DNS Zone                   | <input type="text" value="Google"/>                                  |
| Domain Name                | <input type="text" value="google.com"/>                              |
| Hostname of Primary Master | <input type="text" value="dns"/>                                     |
| Contact Email Address      | <input type="text" value="hostmaster"/>                              |
| TTL (seconds)              | <input type="text" value="86400"/> (range: 0 to 2147483647)          |
| Authoritative              | <input type="button" value="Disable"/>                               |

Under **DNS Entries**, select **Create New**.

Set **Type** to **Address (A)**, set **Hostname** to *www*, and **IP Address** to *216.239.38.120* (the IP address of *forcesafesearch.google.com*).

Type

Address (A) ▼

Hostname

www

IP Address

216.239.38.120

TTL (seconds)

0

(0 to use Zone TTL)

If required, create additional DNS Database entries for other Google search domains (entry for *www.google.[glossary\_exclude]ca[/glossary\_exclude]* shown).

A list of Google search domains can be found [here](#).

Type

☒ Master ☐ Slave

View

☐ Public ☒ Shadow

DNS Zone

Google Canada

Domain Name

google.ca

Hostname of Primary Master

dns

Contact Email Address

hostmaster

TTL (seconds)

86400

(range: 0 to 2147483647)

Authoritative

Disable ▼

DNS Entries

Create New

Edit

Delete

|                          | # | Type        | Details               |
|--------------------------|---|-------------|-----------------------|
| <input type="checkbox"/> | 1 | Address (A) | www -> 216.239.38.120 |

**The network uses an external DNS server**

Using this method will cause your FortiGate to intercept all DNS queries. Because all DNS traffic will be forwarded to the FortiGate internal DNS Service, there might be a performance impact on the FortiGate.

Go to **System > Config > Features** and select **Show More**. Make sure that **DNS Database** is **ON**. If necessary, **Apply** your changes.

DNS Database ?

ON

Go to **System > Network > Interfaces** and create an interface to be used for the FortiGate DNS service.

Set **Type** to **Loopback Interface** and assign an **IP/Network Mask** (in the example, *10.10.10.10/255.255.255.255*).

Interface Name

dns-loopback

Type

Loopback Interface

IP/Network Mask

10.10.10.10/255.255.255.255

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ Auto IPsec Request

Security Mode

None

Enable Explicit Web Proxy

☐

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

☐

Comments

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**:

```
config system dns-server
edit dns-loopback
set mode recursive
end
```

Go to **System > Network > DNS Servers**. The new server is listed under **DNS Service on Interface**.

| DNS Service on Interface |              |           |
|--------------------------|--------------|-----------|
|                          |              |           |
| <input type="checkbox"/> | Interface    | Mode      |
| <input type="checkbox"/> | dns-loopback | Recursive |

Under **DNS Database**, select **Create New**.

Set **DNS Zone** as *Google*, **Domain Name** to *google.com*, and disable **Authoritative**.

Type

☒ Master ☐ Slave

View

☐ Public ☒ Shadow

DNS Zone

Google

Domain Name

google.com

Hostname of Primary Master

dns

Contact Email Address

hostmaster

TTL (seconds)

86400

(range: 0 to 2147483647)

Authoritative

Disable

Under **DNS Entries**, select **Create New**.

Set **Type** to **Address (A)**, set **Hostname** to *www*, and **IP Address** to *216.239.38.120* (the IP address of *forcesafesearch.google.com*).

Type

Address (A)

Hostname

www

IP Address

216.239.38.120

TTL (seconds)

0

(0 to use Zone TTL)



If required, create additional DNS Database entries for other Google search domains (entry for `www.google.ca` shown).

A list of Google search domains can be found [here](#).

Type

☒ Master☐ Slave

View

☐ Public☒ Shadow

DNS Zone

Google Canada

Domain Name

google.ca

Hostname of Primary Master

dns

Contact Email Address

hostmaster

TTL (seconds)

86400

(range: 0 to 2147483647)

Authoritative

Disable

DNS Entries

Create New

Edit

Delete

|  | # | Type        | Details               |
|--|---|-------------|-----------------------|
|  | 1 | Address (A) | www -> 216.239.38.120 |

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console** to create a new virtual IP:

Set **src-filter** to the IP range of your internal users (in the example, `10.10.80.2-10.10.80.100`), **extintf** to your **internal** interface, and **mappedip** to the IP address of the loopback interface.

```
config firewall vip
edit "dns-vip"
set type load-balance
set src-filter "10.10.80.2-10.10.80.100"
set extip 0.0.0.0-239.255.255.255
set extintf internal
set portforward enable
set mappedip "10.10.10.10"
set protocol udp
set extport 53
set mappedport 53
set arp-reply disable
end
```

Go to **Policy & Objects > Policy > IPv4** and create a policy to use the virtual IP to intercept DNS queries.

Set the **Incoming Interface** to your **internal** interface, the **Outgoing Interface** to the loopback interface, **Destination Address** to the virtual IP, and **Service** to **DNS**. Make sure **NAT** is disabled.

Incoming Interface

internal

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

dns-loopback

Destination Address

dns-vip

Schedule

always

Service

DNS

Action

ACCEPT

Firewall / Network Options

OFF

NAT

Select the **Global View** of the policy list. Make sure that the new policy is located above the policy that allows connections from the internal network to the Internet.

| Seq.# | From | To           | Source | Destination | Schedule | Service | Action | NAT     | Web Filter |
|-------|------|--------------|--------|-------------|----------|---------|--------|---------|------------|
| 1     | lan  | dns-loopback | all    | dns-vip     | always   | DNS     | ACCEPT | Disable |            |
| 2     | lan  | wan1         | all    | all         | always   | ALL     | ACCEPT | Enable  | default    |
| 3     | any  | any          | all    | all         | always   | ALL     | DENY   |         |            |

## Results

If you are using full SSL inspection, go to **google.com** and attempt to search for adult/mature content. When the results are shown, a message appears stating that SafeSearch is turned on. This cannot be undone.

If you are using Google Chrome for Internet browsing, you may need to disable SPDY protocol in order for SafeSearch to turn on automatically.

If you have altered the DNS settings, go to **google.com**. A message at the top of the page states that your network has turned on SafeSearch.

Google

porn

Web

Videos

Images

News

Maps

More

Search tools

About 187,000,000 results (0.16 seconds)

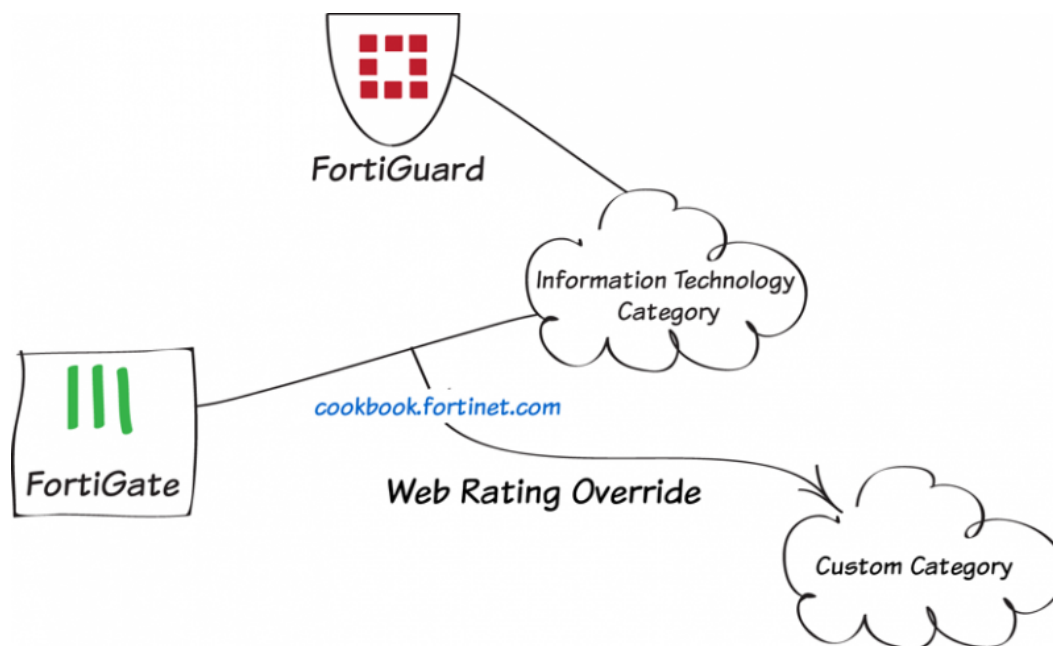
Explicit results filtered with SafeSearch

Learn more

Undo

For further reading, check out [SafeSearch](#)  
and [DNS Services](#) in the [FortiOS 5.2 Handbook](#).

# Web rating overrides



In this recipe, you will change a website's FortiGuard web rating.

*An active license for FortiGuard Web Filtering Services is required to use web ratings.*

For testing purposes, the Cookbook website ([cookbook.fortinet.com](https://cookbook.fortinet.com)) will be changed from the category **Information Technology** to a custom category named **Allowed Sites**.

By changing the web rating for a website, you can control access to the site without affecting the rest of the sites in its original category.

This recipe only changes the website's rating on your FortiGate. To request that the rating is changed for all of FortiGuard, go [here](#).

A video of this recipe is available [here](#).

## 1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.



## 2. Creating a custom category and web rating override

Go to **Security Profiles > Advanced > Web Rating Overrides** and select **Custom Categories**.

Create a new category named *Allowed Sites*.

| + Create New   Edit   Delete |                         |   |
|------------------------------|-------------------------|---|
| Name                         | Number of Override URLs | Number of Web Filter Profile References |
| custom1                      | 0                       | 0                                       |
| custom2                      | 0                       | 0                                       |
| Allowed Sites                | 0                       | 0                                       |

Go to **Security Profiles > Advanced > Web Rating Overrides** and create a new override.

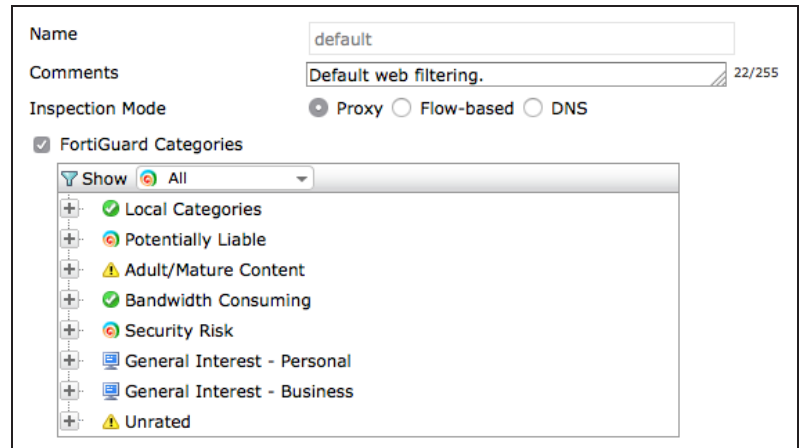
Enter the website's **URL** and select **Lookup Rating** to see the current rating.

In the **Override to** section, set **Category** to **Custom Categories** and **Sub-category** to **Allowed Sites**.

|                                       |  |                      |
|---------------------------------------|--|----------------------|
| URL                                   | <input type="text" value="cookbook.fortinet.com"/> | <b>Lookup Rating</b> |
| <b>FortiGuard Rating</b>              |  |                      |
| Category: General Interest - Business |  |                      |
| Sub-Category: Information Technology  |  |                      |
| <b>Override to</b>                    |  |                      |
| Category                              | <input type="text" value="Custom Categories"/>     |                      |
| Sub-Category                          | <input type="text" value="Allowed Sites"/>         |                      |

### 3. Adding FortiGuard blocking to the default web filter profile

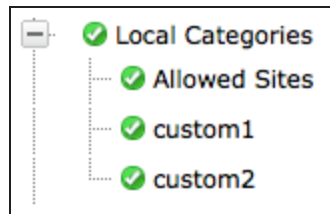
Go to **Security Profiles > Web Filter** and edit the default profile. Enable **FortiGuard Categories**.



The screenshot shows the configuration page for the 'default' web filter profile. The 'Name' field is 'default' and the 'Comments' field is 'Default web filtering.' with a character count of 22/255. The 'Inspection Mode' is set to 'Proxy'. The 'FortiGuard Categories' checkbox is checked. Below this, a list of categories is shown with expand/collapse icons to the left. The categories are: Local Categories (expanded), Potentially Liable, Adult/Mature Content, Bandwidth Consuming, Security Risk, General Interest - Personal, General Interest - Business, and Unrated.

|                             |   |
|-----------------------------|---|
| Name                        | default   |
| Comments                    | Default web filtering. 22/255   |
| Inspection Mode             | <input checked="" type="radio"/> Proxy <input type="radio"/> Flow-based <input type="radio"/> DNS |
| FortiGuard Categories       | <input checked="" type="checkbox"/>   |
| Show All                    |   |
| Local Categories            | ✓   |
| Potentially Liable          | ⚠   |
| Adult/Mature Content        | ⚠   |
| Bandwidth Consuming         | ✓   |
| Security Risk               | ⚠   |
| General Interest - Personal | 📄   |
| General Interest - Business | 📄   |
| Unrated                     | ⚠   |

Expand **Local Categories** to make sure that the **Allowed Sites** category is set to **Allow**.



The screenshot shows the expanded 'Local Categories' list. It contains four items: 'Local Categories' (expanded), 'Allowed Sites', 'custom1', and 'custom2'. Each item has a green checkmark icon to its left, indicating it is set to 'Allow'.

|                  |   |
|------------------|---|
| Local Categories | ✓ |
| Allowed Sites    | ✓ |
| custom1          | ✓ |
| custom2          | ✓ |

Expand **General Interest - Business**.  
Right-click on **Information Technology**  
to set it to **Block**.



#### 4. Adding the default web filter profile to a security policy

Go to **Policy & Objects > Policy > IPv4**  
and edit the policy that allows  
connections from the internal network to  
the Internet.

Under **Security Profiles**, turn on **Web  
Filter** and use the **default** profile.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | lan             |
| Source Address      | all             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address | all             |
| Schedule            | always          |
| Service             | A always        |
| Action              | ACCEPT          |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

**Security Profiles**

☐ AntiVirus

☒ Web Filter

☐ Application Control

☐ IPS

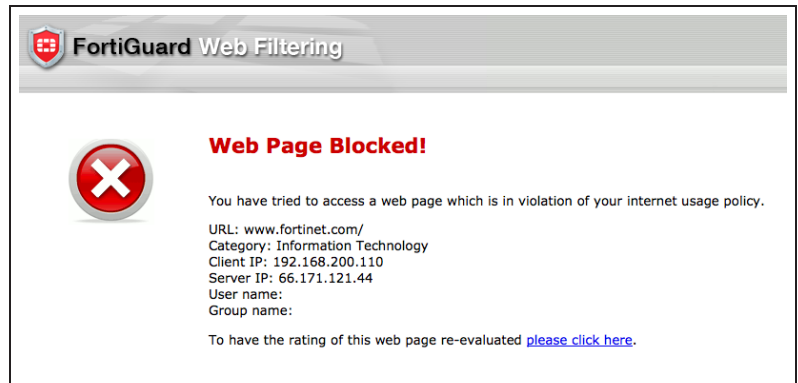
☐ DLP Sensor

Proxy Options

☒ SSL/SSH Inspection

## 5. Results

Browse to [www.fortinet.com](http://www.fortinet.com), which is part of the **Information Technology** category. A message will appear from FortiGuard, stating that access to this website is blocked.

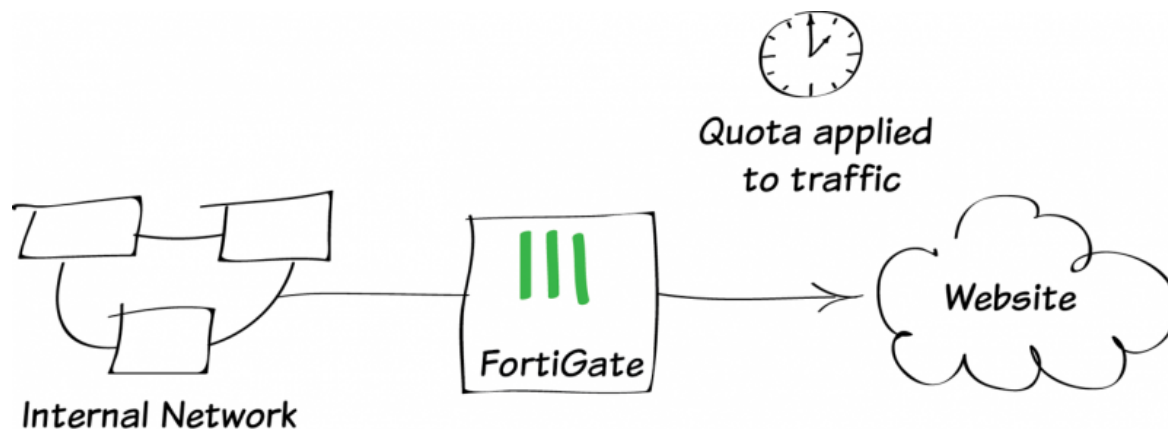


If you browse to [cookbook.fortinet.com](http://cookbook.fortinet.com), you will still be able to access the site.

For further reading, check out **FortiGuard Web Filtering Service** in the **FortiOS 5.2 Handbook**.



# Web filtering using quotas



In this example, you will create a web filter profile that allows access to websites that are categorized as "Personal Interest" at any point during the day, but limits access for a total of 5 minutes for each user.

*An active license for FortiGuard Web Filtering Services is required to use web filtering with quotas.*

Quotas are the most efficient way of allowing limited access to websites, as they do not require set schedules. To apply web filtering using quotas, you must use a security policy with either user or device authentication. In this recipe, a user account, *alistair*, has already been configured. For more information about creating user accounts, see [User and device authentication](#).

A video of this recipe is available [here](#).

## 1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.

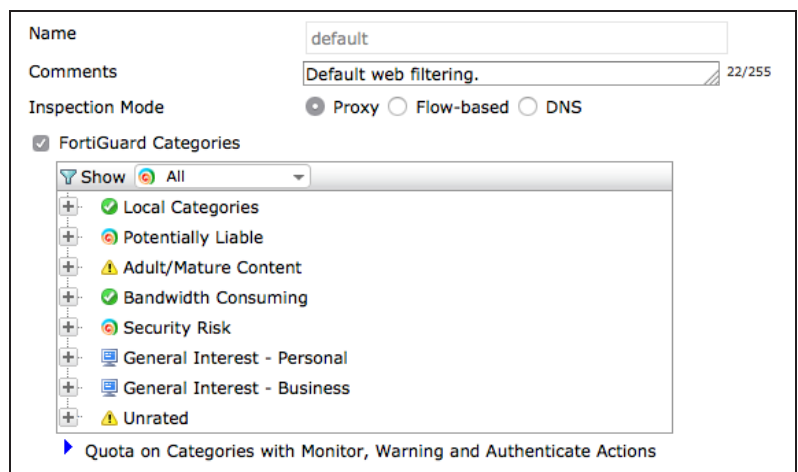


## 2. Creating a web filter profile that uses quotas

Go to **Security Profiles > Web Filter > Profiles**. Edit the **default** profile and enable **FortiGuard Categories**.

Right-click on the category **General Interest - Personal** and select **Monitor**. Do the same for the category **General Interest - Business**.

These categories include a variety of sites that are commonly blocked in the workplace, such as games, instant messaging, and social media.



Expand **Quota on Categories with Monitor, Warning and Authenticate Actions** and select **Create New**.

Select both **General Interest - Personal** and **General Interest - Business**. For testing purposes, set the **Quota** amount to **5 Minutes**.

New/Edit Quota

Potentially Liable

Adult/Mature Content

General Interest - Personal

General Interest - Business

Unrated

Quota

5

Minute(s)

OK

Cancel

The web filter will now list all the sub-categories listed in the two categories and the applied quota.

▼ Quota on Categories with Monitor, Warning and Authenticate Actions

Create New

Edit

Delete

| Category  | Quota |
|---|-------|
| Advertising, Arts and Culture, Brokerage and Trading, Child Education, Content Servers, Digital Postcards, Domain Parking, Dynamic Content, Education, Entertainment, Folklore, Games, Global Religion, Health and Wellness, Instant Messaging, Job Search, Meaningless Content, Medicine, News and Media, Newsgroups and Message Boards, Personal Privacy, Personal Vehicles, Personal Websites and Blogs, Political Organizations, Real Estate, Reference, Restaurant and Dining, Shopping and Auction, Social Networking, Society and Lifestyles, Sports, Travel, Web Chat, Web-based Email, Armed Forces, Business, Finance and Banking, General Organizations, Government and Legal Organizations, Information Technology, Information and Computer Security, Search Engines and Portals, Secure Websites, Web Hosting, Web-based Applications | 5 min |

### 3. Adding web filtering to a security policy with user authentication

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Web Filter** and use the **default** profile.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | lan             |
| Source Address      | all             |
| Source User(s)      | alistair        |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address | all             |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address☐ Fixed Port☐ Use Dynamic IP Pool

☐ Click to add...

**Security Profiles**

☐ AntiVirus

default

☒ Web Filter

default

☐ Application Control

default

☐ IPS

default

☐ DLP Sensor

default

Proxy Options

default

☒ SSL/SSH Inspection

certificate-inspection

### 4. Results

Browse to [www.ebay.com](http://www.ebay.com), a website that is found within the General Interest - Personal category.

Access to the website is allowed for 5 minutes, after which a block message appears. The message will persist for all General Interest - Personal sites until the quota is reset, which occurs every 24 hours at midnight.

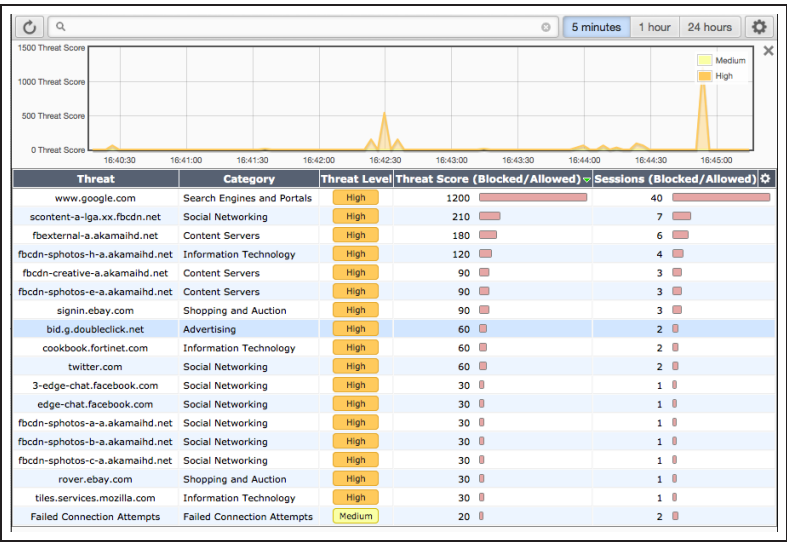
**Web Page Blocked**

Your daily quota for this category of webpage has expired, in accordance with your internet usage policy.

URL: [signin.ebay.com/](http://signin.ebay.com/)  
Category: Shopping and Auction

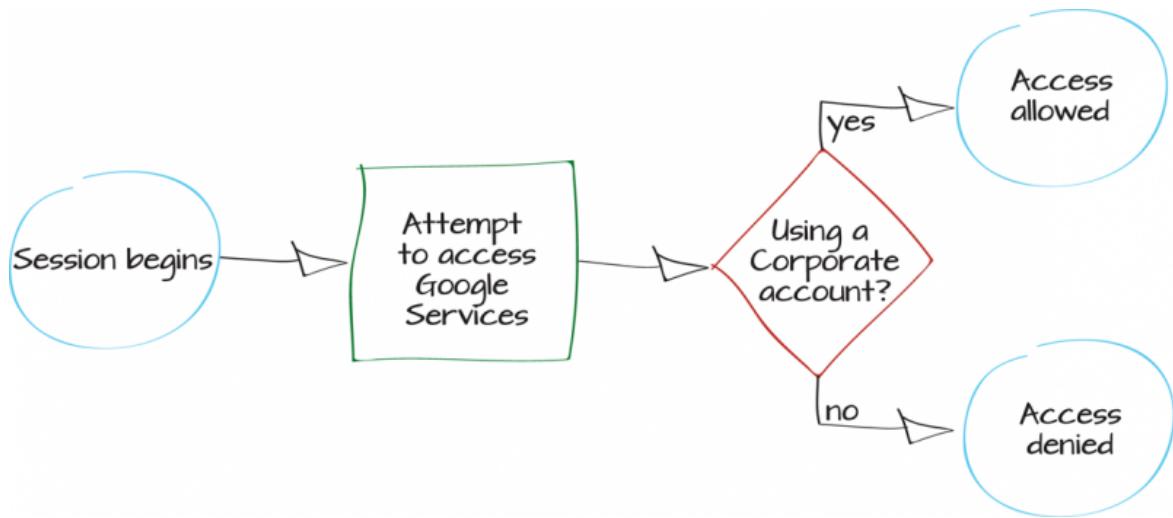
To have the rating of this web page re-evaluated [please click here](#).

Go to **System > FortiView > Threats** and select the **5 minutes** view. You will be able to see the blocked traffic.



For further reading, check out **FortiGuard Web Filtering Service** in the **FortiOS 5.2 Handbook**.

# Blocking Google access for consumer accounts



In this recipe, you will block access to Google services for consumer accounts, while allowing access for corporate accounts.

If your organization has set up a Google corporate account to be able to use Google services, such as Gmail and Google Docs, this recipe can be used to block users from accessing those services with their own personal accounts. In this example, a corporate account has been created that uses the domain *fortidocs.com*.

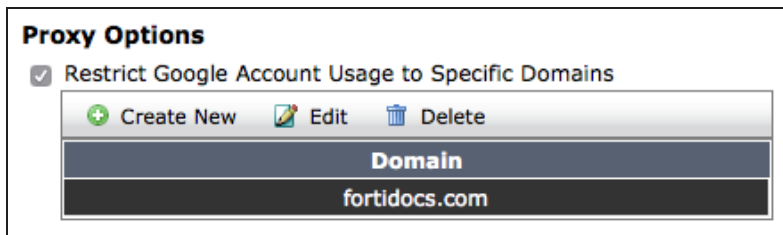
A video of this recipe is available [here](#).

## 1. Editing the default web filter profile to restrict Google access

Go to **Security Profiles > Web Filter** and edit the default profile.

Make sure that **Inspection Mode** is set to **Proxy**. Under **Proxy Options**, select **Restrict Google Account Usage to Specific Domains**.

Select **Create New** in the list that appears and add an entry for the domains for your Corporate Google accounts (in the example, *fortidocs.com*).

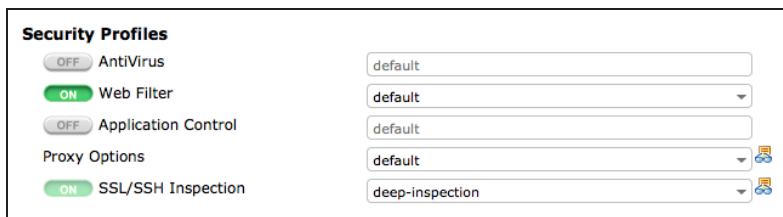


## 2. Adding the profile to your Internet-access policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Enable **Web Filter** and set it to use the **default** profile. Doing this will automatically enable **SSL/SSH Inspection**. Set this to use the **deep-inspection** profile.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).



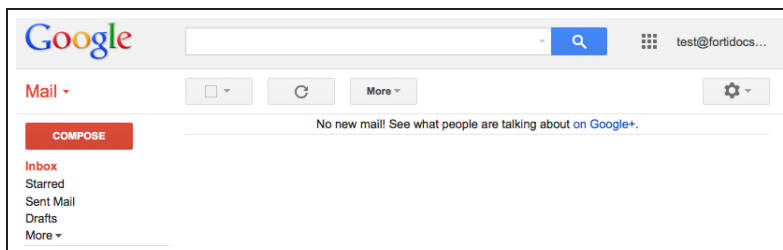
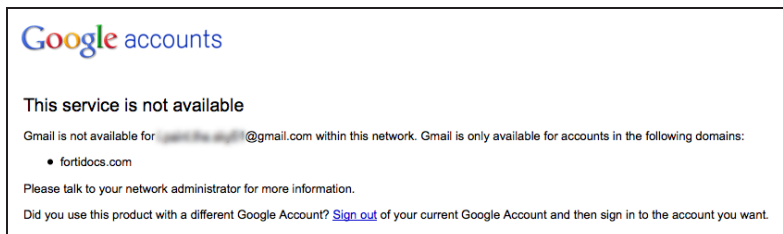
### 3. Results

Log in to Google using a personal account. After you are authenticated, attempt to access a Google service, such as **Gmail** or **Google Drive**.

A message appears from Google stating that the service is not available.

Sign out of the personal account and instead use your corporate account (in the example, *test@fortidocs.com*).

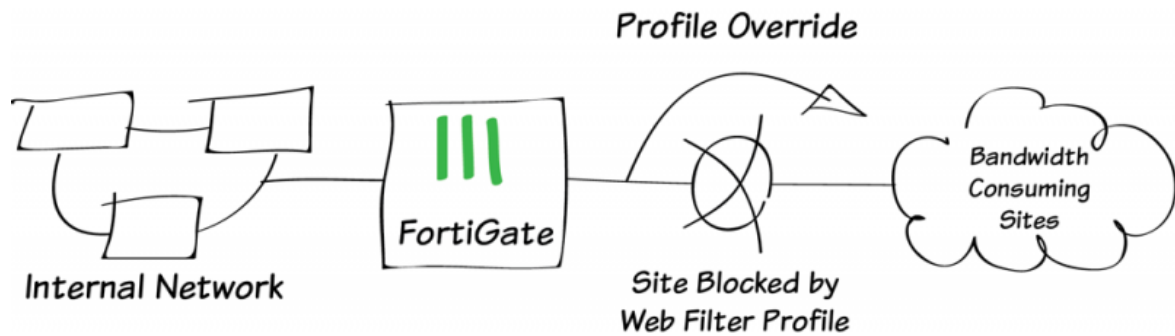
You can now access the Google service.



For further reading, check out **Web filter** in the **FortiOS 5.2 Handbook**.



# Overriding a web filter profile



In this example, one user is temporarily allowed to override a web filter profile to be able to access sites that would otherwise be blocked.

In this example, web filtering blocks the **Bandwidth Consuming** category for all users, except those who can override the filter.

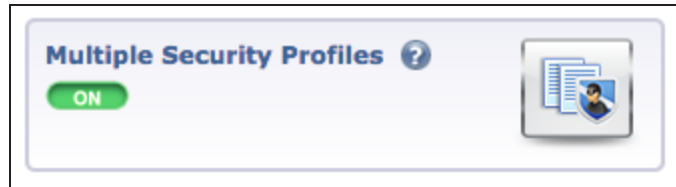
## 1. Enabling web filtering and multiple profiles

Go to **System > Config > Features** and make sure that **Web Filter** is turned **ON**.



Select **Show More** and enable **Multiple Security Profiles**.

**Apply** the changes.



## 2. Creating a user group and two users

Go to **User & Device > User > User Groups**. Create a new group for users who can override web filtering (in the example, *web-filter-override*).

|               |   |
|---------------|---|
| Name          | <input type="text" value="web-filter-override"/>  |
| Type          | <input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input type="radio"/> RADIUS Single Sign-On (RSSO) |
| Members       | <input type="text" value="Click to add..."/>  |
| Remote groups |   |

Go to **User & Device > User > User Definition** and create two users (in the example, *ckent* and *bwayne*).

1 User Type

2 Login Credentials

3 Contact Info

4 Extra Info

☒ Local User  
☐ Remote RADIUS User  
☐ Remote TACACS+ User  
☐ Remote LDAP User

< Back

Next >

Cancel

☒ User Type
 ☒ 2 Login Credentials
 ☐ 3 Contact Info
 ☐ 4 Extra Info

User Name:

Password:

☒ User Type
 ☒ Login Credentials
 ☒ 3 Contact Info
 ☐ 4 Extra Info

Email Address:

☐ SMS

Assign *ckent* to the *web-filter-override* group, but not *bwayne*.

☒ User Type
 ☒ Login Credentials
 ☒ Contact Info
 ☒ 4 Extra Info

☒ Enable

☐ Two-factor Authentication

☒ User Group:

### 3. Creating a web filter profile and override

Go to **Security Profiles > Web Filter** and create a new profile (in the example, *block-bandwidth-consuming*).

Enable FortiGuard Categories, then right-click **Bandwidth Consuming** and select **Block**.

Name:

Comments:

Inspection Mode: ☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show:

- ☒ Local Categories
- ☒ Potentially Liable
- ☒ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☒ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☒ Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

Go to **Security Profiles > Advanced > Web Profile Overrides** and create a new override.

Set **Scope Range** to **User Group**, **User Group** to the *web-filter-override* group, **Original Profile** to the *block-bandwidth-consuming* profile, and **New Profile** to the **default** profile.

Set an appropriate **Expires** time to control how long the override can be used (in the example, *100 hours* after the override is created).

|                  |   |
|------------------|---|
| Scope Range      | <input type="radio"/> User <input checked="" type="radio"/> User Group <input type="radio"/> Source IP  |
| User Group       | <input type="text" value="web-filter-override"/>  |
| Original Profile | <input type="text" value="block-bandwidth-consuming"/>  |
| New Profile      | <input type="text" value="default"/>  |
| Expires          | <input type="text" value="100"/> Days <input type="text" value="0"/> Hours <input type="text" value="0"/> Minutes<br>(Expires: 7/18/2015, 2:57:00 PM) |

## 4. Adding the new web filter profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Source User(s)** to allow both the *web-filter-override* group and user *bwayne*.

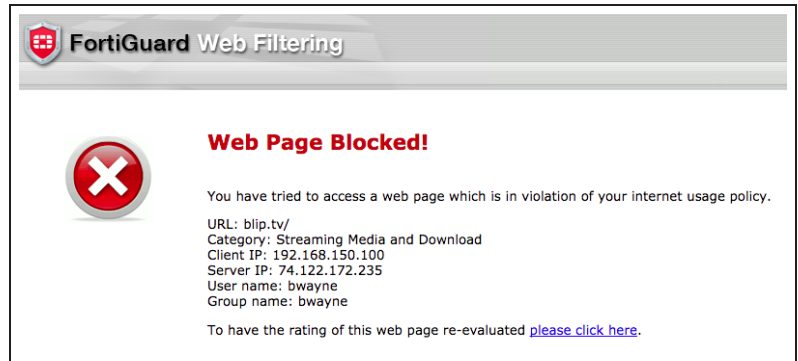
Under **Security Profiles**, turn on **Web Filter** and use the new profile.

|   |   |  |
|---|---|--|
| Incoming Interface  | <input type="text" value="lan (VLAN ID: 0)"/>   |  |
| Source Address  | <input type="text" value="all"/>  |  |
| Source User(s)  | <input type="text" value="web-filter-override"/><br><input type="text" value="bwayne"/> |  |
| Source Device Type  | <input type="text" value="Click to add..."/>  |  |
| Outgoing Interface  | <input type="text" value="wan1"/>   |  |
| Destination Address   | <input type="text" value="all"/>  |  |
| Schedule  | <input type="text" value="always"/>   |  |
| Service   | <input type="text" value="ALL"/>  |  |
| Action  | <input type="text" value="ACCEPT"/>   |  |
| <b>Firewall / Network Options</b>   |   |  |
| <input checked="" type="checkbox"/> NAT   |   |  |
| <input checked="" type="radio"/> Use Outgoing Interface Address <input type="checkbox"/> Fixed Port |   |  |
| <input type="radio"/> Use Dynamic IP Pool <input type="text" value="Click to add..."/>              |   |  |
| <b>Security Profiles</b>  |   |  |
| <input type="checkbox"/> AntiVirus  | <input type="text" value="default"/>  |  |
| <input checked="" type="checkbox"/> Web Filter  | <input type="text" value="block-bandwidth-consuming"/>                                  |  |
| <input type="checkbox"/> Application Control  | <input type="text" value="default"/>  |  |
| Proxy Options   | <input type="text" value="default"/>  |  |
| <input checked="" type="checkbox"/> SSL/SSH Inspection  | <input type="text" value="certificate-inspection"/>                                     |  |

## 5. Results

Browse to **blip.tv**, a website that is part of the **Bandwidth Consuming** category.

Authenticate using the *bwayne* account.  
The website is blocked.



Go to **User & Device > Monitor > Firewall** and **De-authenticate** *bwayne*.

Browse to blip.tv again, this time authenticating using the *ckent* account. You can access the website until the override expires.

For further reading, check out **Web Filter** in the **FortiOS 5.2 Handbook**.

# Troubleshooting web filtering

This section contains tips to help you with some common challenges of FortiGate web filtering.

## The Web Filter option does not appear in the GUI.

Go to **Config > System > Features** and enable **Web Filter**.

## New Web Filter profiles cannot be created.

Go to **Config > System > Features** and select **Show More**. Enable **Multiple Security Profiles**.

## Web Filtering has been configured but is not working.

Make sure that web filtering is enabled in a policy. If it is enabled, check that the policy is the policy being used for the correct traffic. Also check that the policy is getting traffic by going to the policy list and adding the Sessions column to the list.

## An active FortiGuard Web Filtering license displays as expired/unreachable.

First, ensure that web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

If web filtering is enabled in a policy, go to **System > Config > FortiGuard** and expand **Web Filtering**. Under **Port Selection**, select **Use Alternate Port (8888)**. Select **Apply** to save the changes. Check whether the license is shown as active. If it is still inactive/expired, switch back to the default port and check again.

# VPNs

This section contains information about configuring a variety of different Virtual Private Networks (VPNs), as well as different methods of authenticating VPN users. FortiGates support two types of VPNs: IPsec and SSL.

IPsec VPNs use Internet Protocol Security (IPsec) to create a VPN that extends a private network across a public network, typically the Internet. In order to connect to an IPsec VPN, users must install and configure an IPsec VPN client (such as FortiClient) on their PCs or mobile devices.

SSL VPNs use Secure Sockets Layer (SSL) to create a VPN that extends a private network across a public network, typically the Internet. Connections to an SSL VPN are done through a web browser and do not require any additional applications.

## IPsec

- [IPsec VPN with FortiClient](#)
- [IPsec VPN for iOS devices](#)
- [IPsec VPN with the native Mac OS client](#)
- [IPsec VPN with two-factor authentication](#)
- [IPsec VPN with external DHCP service](#)
- [Site-to-site IPsec VPN with two FortiGates](#)
- [Site-to-site IPsec VPN with overlapping subnets](#)
- [IPsec VPN to Microsoft Azure](#)
- [Remote Internet browsing using a VPN](#)
- [Remote browsing using site-to-site IPsec VPN](#)
- [IPsec troubleshooting](#)

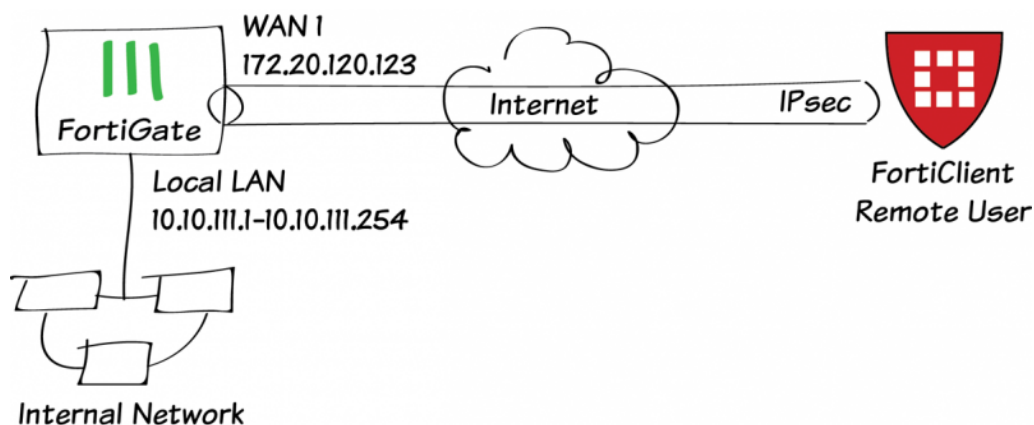
## SSL

- [SSL VPN for remote users](#)
- [SSL VPN using FortiClient for iOS](#)
- [SSL VPN for Windows Phone 8.1](#)
- [Remote Internet browsing using a VPN](#)
- [SSL VPN with certificate authentication](#)
- [RADIUS authentication for SSL VPN with FortiAuthenticator](#)
- [LDAP authentication for SSL VPN with FortiAuthenticator](#)
- [SSL VPN remote browsing with LDAP authentication](#)

- SMS two-factor authentication for SSL VPN
- SSL VPN troubleshooting



# IPsec VPN with FortiClient



This recipe uses the IPsec VPN Wizard to provide a group of remote users with secure, encrypted access to the corporate network.

The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet. When the tunnel is configured, you will connect using the FortiClient application.

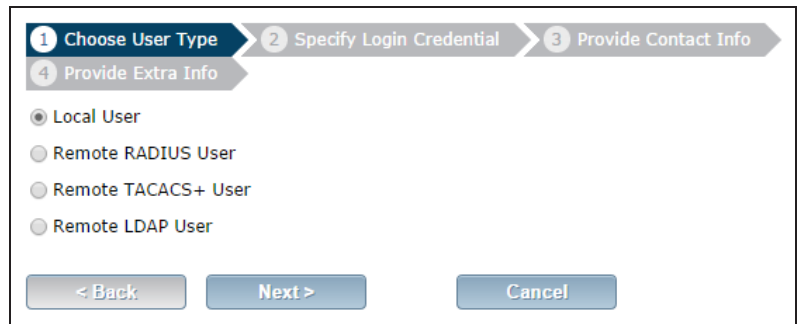
A video of this recipe is available [here](#).

## 1. Creating a user group for remote users

Go to **User & Device > User > User Definition**.

Create a new **Local User** with the **User Creation Wizard**.

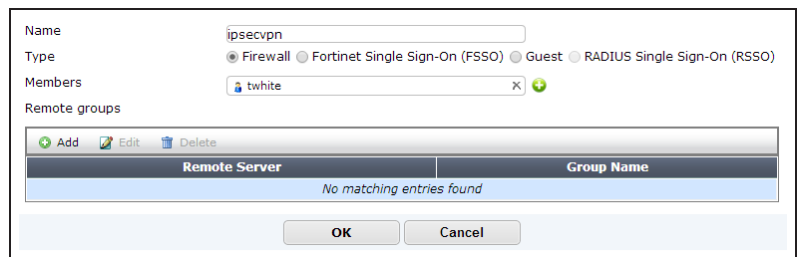
Proceed through each step of the wizard, carefully entering the appropriate information.



The screenshot shows the first step of the User Creation Wizard. At the top, there are four numbered steps: 1. Choose User Type (active), 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info. Below the steps, there are four radio button options: Local User (selected), Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. At the bottom, there are three buttons: < Back, Next >, and Cancel.

Go to **User & Device > User > User Groups**.

Create a user group for remote users and add the user you created.



The screenshot shows the User Groups configuration form. The Name field is set to 'ipsecvpn'. The Type field has four radio button options: Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO). The Members field contains 'twhite'. Below the Members field is a section for Remote groups with a table. The table has two columns: Remote Server and Group Name. The table is currently empty, showing 'No matching entries found'. At the bottom, there are OK and Cancel buttons.

## 2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add a firewall address for the Local LAN, including the subnet and local interface.



The screenshot shows the Address configuration form. The Category field has three radio button options: Address (selected), IPv6 Address, and Multicast Address. The Name field is set to 'Local LAN'. The Type field is set to 'Subnet'. The Subnet / IP Range field is set to '10.10.111.0/255.255.255.0'. The Interface field is set to 'port1'. The Visibility field is checked. The Comments field is set to 'Write a comment...'. At the bottom, there are OK and Cancel buttons.

### 3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click Next.

*The tunnel name may not have any spaces in it.*

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Client Options

Name:

Template:

- ☒ Dialup - FortiClient (Windows, Mac OS, Android)
- ☐ Site to Site - FortiGate
- ☐ Dialup - iOS (Native)
- ☐ Dialup - Android (Native L2TP/IPsec)
- ☐ Dialup - Cisco Firewall
- ☐ Site to Site - Cisco
- ☐ Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the new user group, then click **Next**.

*The pre-shared key is a credential for the VPN and should differ from the user's password.*

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Client Options

Incoming Interface:

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key:

☒ Hide Characters

User Group:

< Back Next > Cancel

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the \_range suffix (in this case, ipsecvpn\_range).*

*In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.*

Click **Next** and select **Client Options** as desired.

VPN Setup

Authentication

3 Policy & Routing

4 Client Options

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

Local Interface

port1

Local Address

Local LAN

Client Address Range

10.10.111.1-10.10.111.254

Subnet Mask

255.255.255.255

DNS Server

☒ Use System DNS

☐ Specify

☐ Enable IPv4 Split Tunnel

☒ Allow Endpoint Registration

< Back

Next >

Cancel

VPN Setup

Authentication

Policy & Routing

4 Client Options

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

☒ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

< Back

Create

Cancel

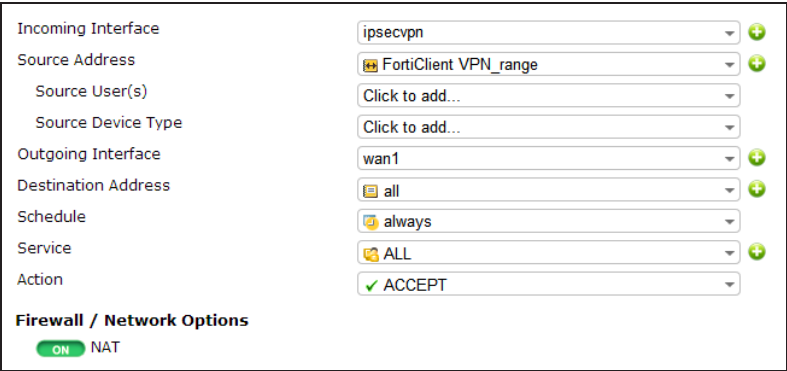
## 4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**. Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.



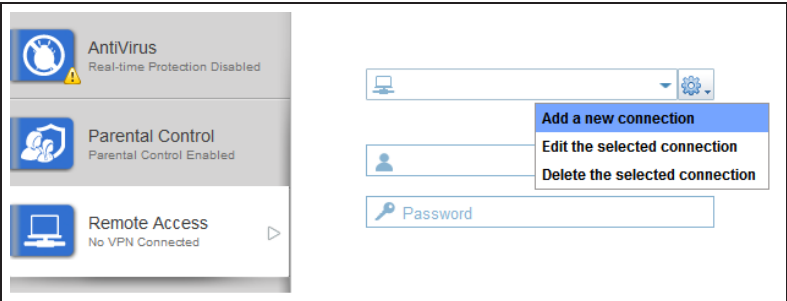
|                     |                       |
|---------------------|-----------------------|
| Incoming Interface  | ipsecvpn              |
| Source Address      | FortiClient VPN_range |
| Source User(s)      | Click to add...       |
| Source Device Type  | Click to add...       |
| Outgoing Interface  | wan1                  |
| Destination Address | all                   |
| Schedule            | always                |
| Service             | ALL                   |
| Action              | ACCEPT                |

**Firewall / Network Options**

☒ ON NAT

## 5. Configuring FortiClient

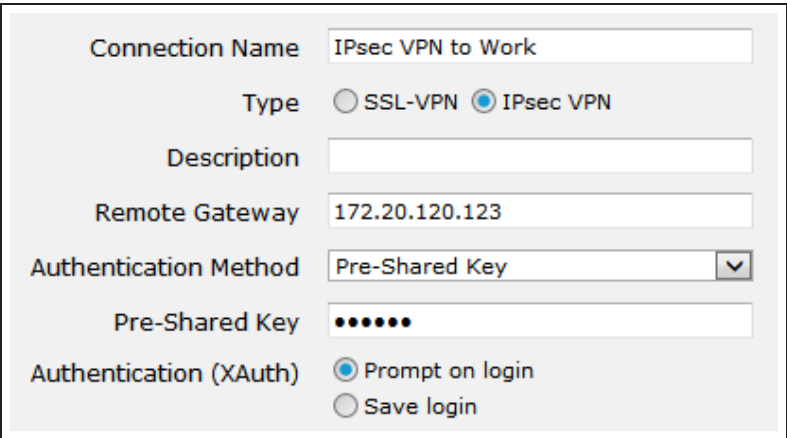
Open FortiClient, go to **Remote Access** and **Add a new connection**.



Provide a **Connection Name** and set the **Type** to **IPsec VPN**.

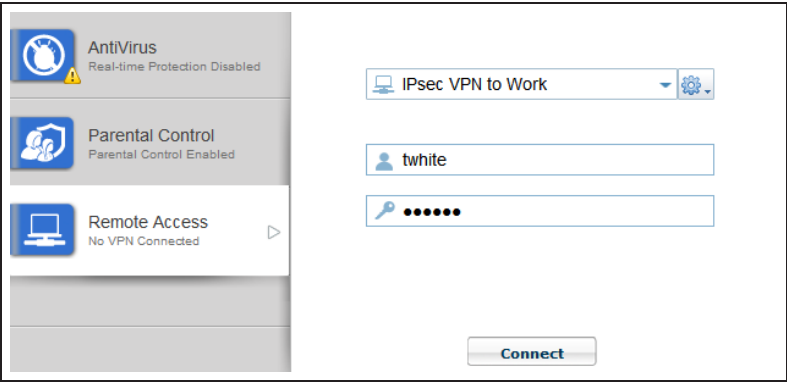
Set **Remote Gateway** to the FortiGate IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key below.



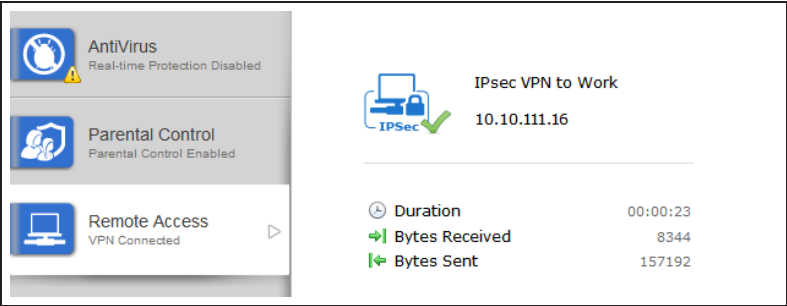
|                        |   |
|------------------------|---|
| Connection Name        | IPsec VPN to Work   |
| Type                   | <input type="radio"/> SSL-VPN <input checked="" type="radio"/> IPsec VPN          |
| Description            |   |
| Remote Gateway         | 172.20.120.123  |
| Authentication Method  | Pre-Shared Key  |
| Pre-Shared Key         | .....   |
| Authentication (XAuth) | <input checked="" type="radio"/> Prompt on login <input type="radio"/> Save login |

Select the new connection, enter the username and password, and click **Connect**.



## 6. Results

Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

| Name    | Ty...  | Remote Gatew... | Stat... | Incoming D... | Outgoing Data |
|---------|--------|-----------------|---------|---------------|---------------|
| ipsec_0 | Dialup | 172.20.120.16   | Up      | 9.22 K        | 3.48 K        |

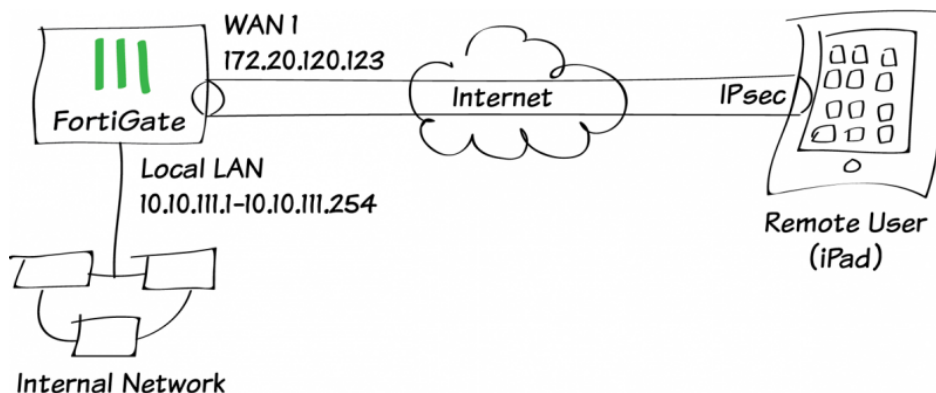
Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

| # | Date/Time | Src Interface | Dst Interface | Src          | Dst           | Sent / Received |
|---|-----------|---------------|---------------|--------------|---------------|-----------------|
| 1 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 59 B / 221 B    |
| 2 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 60 B / 292 B    |
| 3 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 56 B / 288 B    |

Verify that the **Sent/Received** column displays traffic successfully flowing through the tunnel.

For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

# IPsec VPN for iOS devices



This recipe uses the IPsec VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.

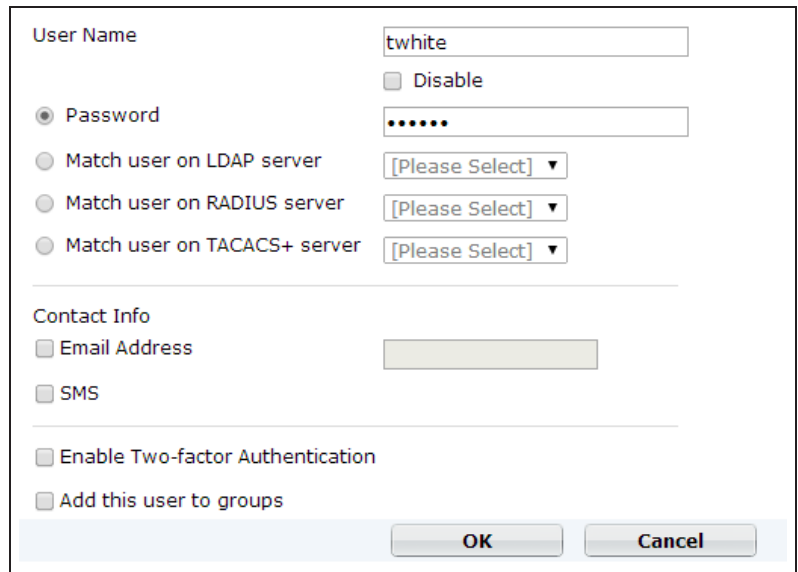
*This recipe was tested using an iPad 2 running iOS version 7.1.*

A video of this recipe can be found [here](#).

## 1. Creating a user group for iOS users

Go to **User & Device > User > User Definition**.

Create a new user.

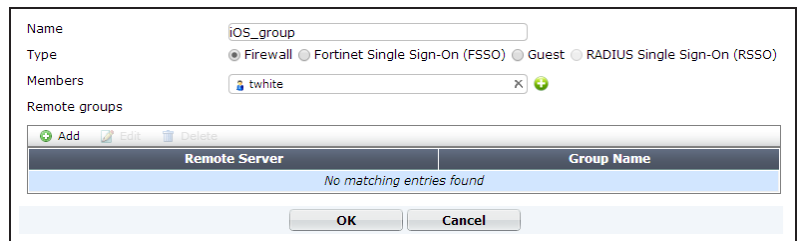


The 'User Definition' form contains the following fields and options:

- User Name:** A text input field containing 'twhite'.
- Disable:** A checkbox that is currently unchecked.
- Password:** A radio button that is selected, followed by a password input field with masked characters (dots).
- Match user on LDAP server:** A radio button that is unselected, followed by a dropdown menu showing '[Please Select]'.
- Match user on RADIUS server:** A radio button that is unselected, followed by a dropdown menu showing '[Please Select]'.
- Match user on TACACS+ server:** A radio button that is unselected, followed by a dropdown menu showing '[Please Select]'.
- Contact Info:**
  - Email Address:** A checkbox that is unchecked, followed by an empty text input field.
  - SMS:** A checkbox that is unchecked.
- Enable Two-factor Authentication:** A checkbox that is unchecked.
- Add this user to groups:** A checkbox that is unchecked.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Go to **User & Device > User > User Groups**.

Create a user group for iOS users and add the user you created.



The 'User Groups' form contains the following fields and options:

- Name:** A text input field containing 'iOS\_group'.
- Type:** Radio buttons for 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', 'Guest', and 'RADIUS Single Sign-On (RSSO)'.
- Members:** A text input field containing 'twhite' with a search icon and a green plus icon.
- Remote groups:** A section with 'Add', 'Edit', and 'Delete' buttons above a table.

| Remote Server             | Group Name |
|---------------------------|------------|
| No matching entries found |            |
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.



## 2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.








Add a firewall address for the Local LAN, including the subnet and local interface.

|  |   |
|--|---|
| Category   | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name   | <input type="text" value="Local LAN"/>  |
| Type   | <input type="text" value="Subnet"/>   |
| Subnet / IP Range  | <input type="text" value="10.10.111.0/255.255.255.0"/>  |
| Interface  | <input type="text" value="port1"/>  |
| Visibility   | <input checked="" type="checkbox"/>   |
| Comments   | <input type="text" value="Write a comment..."/> 0/255   |
| <div><input type="button" value="OK"/> <input type="button" value="Cancel"/></div> |   |

## 3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPsec > Wizard**.

Name the VPN connection and select **Dial Up - iOS (Native)** and click **Next**.

|  |   |
|--|---|
| <div><div>1 VPN Setup</div><div>2 Authentication</div><div>3 Policy &amp; Routing</div></div>  |   |
| Name   | <input type="text" value="iOSvpn_Native"/><br><i>10 concurrent user(s) will be supported</i>  |
| Template   | <div><div> Dialup - FortiClient (Windows, MacOS, Android)</div><div> Site to Site - FortiGate</div><div> Dialup - iOS (Native)</div><div> Dialup - Android (Native L2TP/IPsec)</div><div> Dialup - Cisco Firewall</div><div> Site to Site - Cisco</div><div> Custom VPN Tunnel (No Template)</div></div> |
| <div><div><input type="button" value=" &lt; Back"/></div><div><input type="button" value=" Next &gt;"/></div><div><input type="button" value=" Cancel"/></div></div> |   |

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the iOS user group, then click **Next**.

*The pre-shared key is a credential for the VPN and should differ from the user's password.*

VPN Setup > **2 Authentication** > Policy & Routing

iOSvpn\_native : Dialup - iOS (Native)

Incoming Interface: wan1

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key: ..... ☒ Hide Characters

User Group: iOS\_group

☐ Require 'Group Name' on VPN client

< Back Next > Cancel

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the iOS users address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **\_range** suffix (in this case, **iOSvpn\_Native\_range**).*

*In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.*

VPN Setup > Authentication > **3 Policy & Routing**

iOSIPsecVPN : Dialup - iOS (Native)

Local Interface: port1

Local Address: Local LAN

Client Address Range: 10.10.111.1-10.10.111.254

Subnet Mask: 255.255.255.255

DNS Server: ☒ Use System DNS ☐ Specify

☐ Enable IPv4 Split Tunnel

< Back Create Cancel

## 4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to all.

Set **Outgoing Interface** to **wan1** and **Destination Address** to all.

Set **Service** to **all** and ensure that you enable **NAT**.

|                     |                            |
|---------------------|----------------------------|
| Incoming Interface  | <div>iOSvpn_Native</div>   |
| Source Address      | <div>all</div>             |
| Source User(s)      | <div>Click to add...</div> |
| Source Device Type  | <div>Click to add...</div> |
| Outgoing Interface  | <div>wan1</div>            |
| Destination Address | <div>all</div>             |
| Schedule            | <div>always</div>          |
| Service             | <div>ALL</div>             |
| Action              | <div>ACCEPT</div>          |

**Firewall / Network Options**

ON

 NAT

Use Destination Interface Address

Fixed Port

## 5. Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.

Cancel IPsec VPN 5.2 Save

L2TP PPTP IPsec

Description IPsec VPN 5.2

Server 172.20.120.123

Account twhite

Password ••••••

Use Certificate ☐

Group Name

Secret ••••••

PROXY

Off Manual Auto

## 6. Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

| Name            | Type   | Remote Gateway | Username | Status | Incoming Data | Outgoing Data | Phase 2 Proposal |
|-----------------|--------|----------------|----------|--------|---------------|---------------|------------------|
| iOSvpn_Native_0 | Dialup | 172.20.120.16  |          | Up     | 9.22 K        | 3.48 K        | iOSvpn_Native    |

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

| # | Date/Time | Src Interface | Dst Interface | Src           | Dst           | Sent / Received |
|---|-----------|---------------|---------------|---------------|---------------|-----------------|
| 1 | 11:22:41  | iOSvpn_Native | wan1          | 10.10.111.16  | 208.91.112.53 | 59 B / 221 B    |
| 2 | 11:22:41  | iOSvpn_Native | wan1          | 10.10.111.16  | 208.91.112.53 | 60 B / 292 B    |
| 3 | 11:22:41  | iOSvpn_Native | wan1          | 10.10.111.16  | 208.91.112.53 | 56 B / 288 B    |
| 4 | 11:21:42  | port1         |               | 192.168.1.117 | 208.91.113.70 | 304 B / 304 B   |

Select an entry to view more information.



|                     |               |                     |   |
|---------------------|---------------|---------------------|---|
| Dst                 | 192.168.1.114 | Virtual Domain      | root  |
| Received            | 72            | Source Country      | Reserved  |
| Sent / Received     | 72 B / 72 B   | Duration            | 63  |
| Sent                | 72            | Application Details |   |
| Service             | PING          | Protocol            | 1   |
| Destination Country | Reserved      | roll                | 65428   |
| Status              | ✓             | Timestamp           | Thu Feb 21 11:20:44 2014  |
| Tran Display        | noop          | Sequence Number     | 220067  |
| Policy ID           | 6             | Src Interface       | iOSvpn  |
| Src                 | 10.10.111.16  | VPN                 | iOSvpn_Native   |
| Sent Packets        | 2             | Level               | notice <div><div></div><div></div><div></div><div></div><div></div></div> |
| VPN Type            | ipsec-dynamic | logid               | 13  |
| Sub Type            | forward       | Threat              |   |
| Received Packets    | 2             | Date/Time           | 11:20:44 (Thu Feb 21 11:20:44 2014)                                       |
| Dst Interface       | port1         |                     |   |

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

| Refresh |           | Download Raw Log |               |              |                |                    |
|---------|-----------|------------------|---------------|--------------|----------------|--------------------|
| #       | Date/Time | Src Interface    | Dst Interface | Src          | Dst            | Sent / Received    |
| 1       | 11:28:43  | ios_P1           | wan1          | 10.10.111.16 | 74.121.50.17   | 1023 B / 579 B     |
| 2       | 11:22:41  | iOSvpn_Native    | wan1          | 10.10.111.16 | 208.91.112.53  | 59 B / 221 B       |
| 3       | 11:22:41  | iOSvpn_Native    | wan1          | 10.10.111.16 | 208.91.112.53  | 60 B / 292 B       |
| 4       | 11:22:41  | iOSvpn_Native    | wan1          | 10.10.111.16 | 208.91.112.53  | 56 B / 288 B       |
| 5       | 11:20:42  | iOSvpn_Native    | wan1          | 10.10.111.16 | 173.194.73.105 | 812 B / 642 B      |
| 6       | 11:20:42  | iOSvpn_Native    | wan1          | 10.10.111.16 | 74.125.134.102 | 808 B / 712 B      |
| 7       | 11:20:42  | iOSvpn_Native    | wan1          | 10.10.111.16 | 173.194.73.94  | 2.96 KB / 23.07 KB |
| 8       | 11:20:35  | iOSvpn_Native    | wan1          | 10.10.111.16 | 17.149.36.134  | 104 B / 60 B       |
| 9       | 11:19:15  | iOSvpn_Native    | wan1          | 10.10.111.16 | 204.93.33.67   | 813 B / 365 B      |

Select an entry to view more information.

|                     |  |                     |                                     |
|---------------------|--|---------------------|-------------------------------------|
| Dst                 |  74.121.50.17 | Virtual Domain      | root                                |
| Received            | 579  | Source Country      | Reserved                            |
| Src NAT IP          | 172.20.120.123   | Sent / Received     | 1023 B / 579 B                      |
| Duration            | 2  | Sent                | 1023                                |
| Src NAT Port        | 50189  | Application Details |                                     |
| Service             | HTTP   | Protocol            | 6                                   |
| Destination Country | United States  | Dst Port            | 80                                  |
| roll                | 65428  | Status              | close                               |
| Timestamp           | Thu Feb 21 11:28:43 2014   | Tran Display        | snat                                |
| Sequence Number     | 221594   | Policy ID           | 7                                   |
| Src Interface       | iOSvpn_Native  | Src                 | 10.10.111.16                        |
| VPN                 | iOSvpn   | Sent Packets        | 6                                   |
| Level               | notice        | VPN Type            | ipsec-dynamic                       |
| Src Port            | 50189  | logid               | 13                                  |
| Sub Type            | forward  | Threat              |                                     |
| Received Packets    | 4  | Date/Time           | 11:28:43 (Thu Feb 21 11:28:43 2014) |
| Dst Interface       | wan1   |                     |                                     |

You can also view the status of the tunnel on the iOS device itself.

On the device, go to **Settings > VPN > Status** and view the status of the connection.

|              |                |
|--------------|----------------|
| Server       | 172.20.120.123 |
| Connect Time | 9:48           |
| Connected to | 172.20.120.82  |
| IP Address   | 10.10.111.1    |

Lastly, using a Ping tool, you can send a ping packet from the iOS device directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel.

IP Address to ping:  [Start](#) [Clear](#)

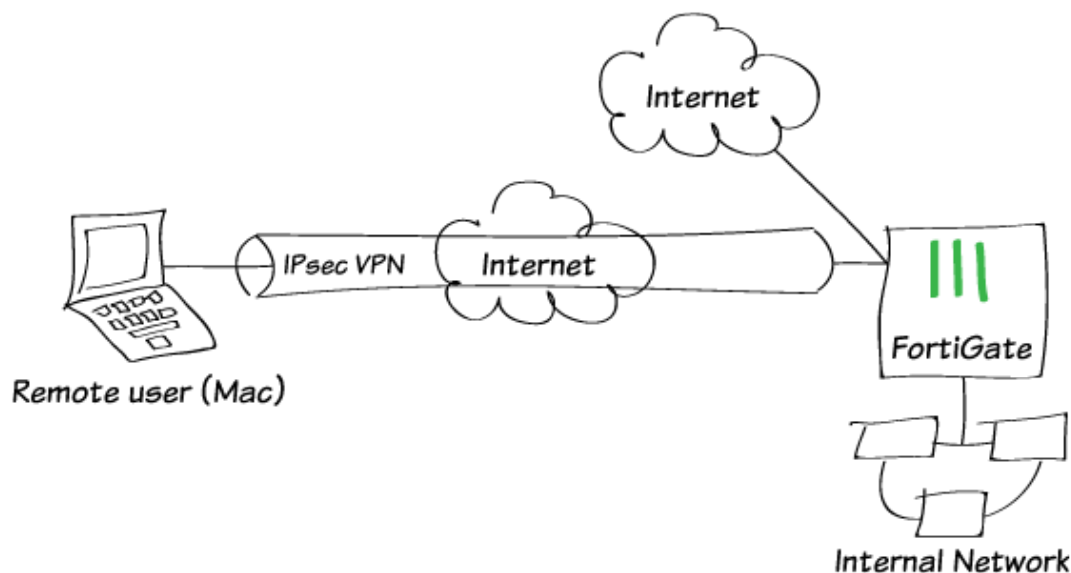
Delay: 2000 ms

Result:

```
PING 172.20.120.123 (172.20.120.123)
36 bytes from 172.20.120.123: icmp_seq=0 ttl=254 time=12 ms
36 bytes from 172.20.120.123: icmp_seq=1 ttl=254 time=5 ms
36 bytes from 172.20.120.123: icmp_seq=2 ttl=254 time=10 ms
36 bytes from 172.20.120.123: icmp_seq=3 ttl=254 time=10 ms
--- 172.20.120.123 ping statistics ---
4 packets transmitted, 4 packets received, lost 0.0 %
```

For further reading, check out [FortiGate dialup-client configurations](#) in the [FortiOS 5.2 Handbook](#).

# IPsec VPN with the native Mac OS client



In this recipe, you will learn how to create an IPsec VPN on a FortiGate, and connect to it using the default client built into the Mac OS.

This VPN configuration allows Mac users to securely access an internal network as well as browse the Internet through the VPN tunnel.

*The recipe assumes that a "mac\_users" user group and a Local LAN firewall address have been created.*

This recipe was tested using Mac OS 10.10.2 (Yosemite).

A video of this recipe is available [here](#).



# 1. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - Cisco Firewall** and click **Next**.

*The native Mac OS client is a Cisco client, which is why you select Dialup - Cisco Firewall in the VPN Wizard.*

1 VPN Setup 2 Authentication 3 Policy & Routing

Name NativeMac

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall**
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key, select the appropriate **User Group**, then click **Next**.

1 VPN Setup 2 Authentication 3 Policy & Routing

NativeMac : Dialup - Cisco Firewall

Incoming Interface wan1

Authentication Method ☒ Pre-shared Key ☐ Signature

Pre-shared Key .....  
☒ Hide Characters

User Group mac\_users

☐ Require 'Group Name' on VPN client

< Back Next > Cancel

Set **Local Interface** to an internal interface and set **Local Address** to the local LAN address.

Enter an IP address range for VPN users in the **Client Address Range** field then click **Next**.

VPN Setup

Authentication

3 Policy & Routing

NativeMac : Dialup - Cisco Firewall

Local Interface

internal1 (Local LAN)

Local Address

Internal

Client Address Range

10.10.10.1-10.10.10.100

Subnet Mask

255.255.255.0

DNS Server

Use System DNS

Specify

Enable IPv4 Split Tunnel

< Back

Create

Cancel

The IPsec VPN Wizard finishes with a summary of created objects.

VPN Setup

Authentication

Policy & Routing

NativeMac : Dialup - Cisco Firewall

The VPN has been set up

Summary of Created Objects

Phase 1 Interface

NativeMac

Phase 2 Interface

NativeMac

Address

NativeMac\_range

Remote to Local Policy

2

Add Another

Show Tunnel List

Go to **Policy & Objects > Objects > Addresses** and confirm that the wizard has created the IPsec VPN firewall address range.

| Name                | Type     | Details                         | Interface | Visibility | Ref. |  |
|---------------------|----------|---------------------------------|-----------|------------|------|--|
| Address (16)        |          |                                 |           |            |      |  |
| Gotomeeting         | FQDN     | *.gotomeeting.com               | Any       | ✓          | 1    |  |
| Internal            | Subnet   | 192.168.1.0/24                  | internal1 | ✓          | 1    |  |
| NativeMac_range     | IP Range | 10.10.10.1 - 10.10.10.100       | Any       | ✓          | 1    |  |
| SSLVPN_TUNNEL_ADDR1 | IP Range | 10.212.134.200 - 10.212.134.210 | Any       | ✓          | 2    |  |
| all                 | Subnet   | 0.0.0.0/0                       | Any       | ✓          | 2    |  |

Go to **Policy & Objects > Policy > IPv4** and confirm that the wizard has created the policy from the VPN tunnel interface to the internal interface.

| Seq.#                                       | Source          | Destination | Schedule | Service | Action   | NAT      |
|---|-----------------|-------------|----------|---------|----------|----------|
| ▶ Internal1 (Local LAN) - wan1 (1 - 1)      |                 |             |          |         |          |          |
| ▼ NativeMac - Internal1 (Local LAN) (2 - 2) |                 |             |          |         |          |          |
| 2   | NativeMac_range | Internal    | always   | ALL     | ✓ ACCEPT | ✓ Enable |
| ▶ Implicit (3 - 3)                          |                 |             |          |         |          |          |

## 2. Creating a security policy for remote access to the Internet

Under **Policy & Objects > Policy > IPv4**, create a security policy

allowing remote users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and **Destination Address** to **all**.

Set **Service** to **ALL** and enable **NAT**.

Incoming InterfaceNativeMac

Source Addressall

Source User(s)Click to add...

Source Device TypeClick to add...

Outgoing Interfacewan1

Destination Addressall

Schedulealways

ServiceALL

Action✓ ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Fixed Port

Use Dynamic IP Pool

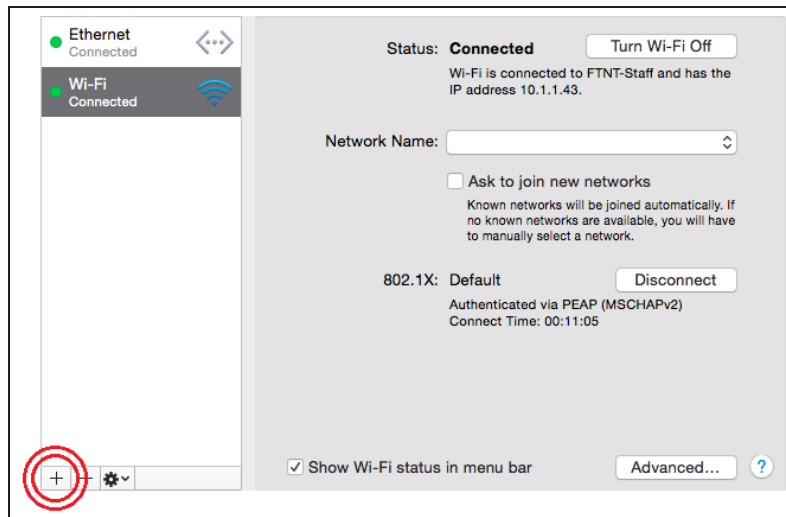
Click to add...

The policy should appear in the policy list at **Policy & Objects > Policy > IPv4**.

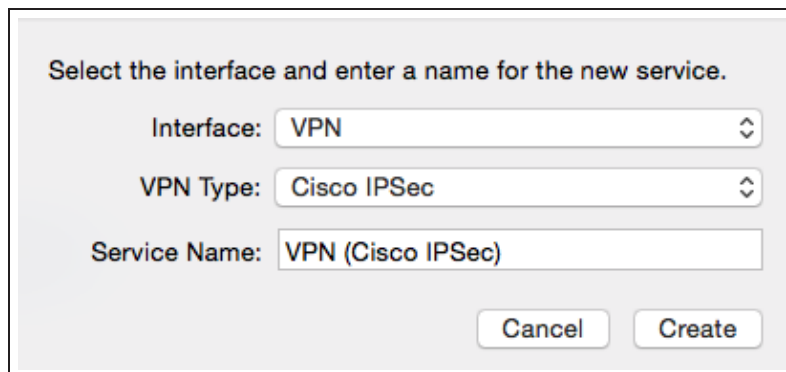
| Seq.#                                       | Source          | Destination | Schedule | Service | Action   | NAT      |
|---|-----------------|-------------|----------|---------|----------|----------|
| ▶ Internal1 (Local LAN) - wan1 (1 - 1)      |                 |             |          |         |          |          |
| ▼ NativeMac - Internal1 (Local LAN) (2 - 2) |                 |             |          |         |          |          |
| 2   | NativeMac_range | Internal    | always   | ALL     | ✓ ACCEPT | ✓ Enable |
| ▼ NativeMac - wan1 (3 - 3)                  |                 |             |          |         |          |          |
| 3   | all             | all         | always   | ALL     | ✓ ACCEPT | ✓ Enable |
| ▶ Implicit (4 - 4)                          |                 |             |          |         |          |          |

### 3. Connecting to the IPsec VPN using the native Mac client

On the Mac, go to **System Preferences** > **Network** and click the **Plus (+)** button.



Set **Interface** to **VPN**, set **VPN Type** to **Cisco IPsec**, and click **Create**.



Set the **Server Address** to the FortiGate IP address, configure the network account details for the remote user, then click **Authentication Settings**.

Ethernet  
Connected

Wi-Fi  
Connected

VPN (C...IPSec)  
Not Configured

+

-

⚙

▼

Status: **Not Configured**

Server Address: 172.20.120.82

Account Name: ckent

Password: ●●●●●●

Authentication Settings...

Connect

☐ Show VPN status in menu bar

Advanced... ?

Select **Shared Secret** and enter the pre-shared key you created **above**, then click **OK**.

Machine Authentication:

☒ Shared Secret: ●●●●●●

☐ Certificate Select...

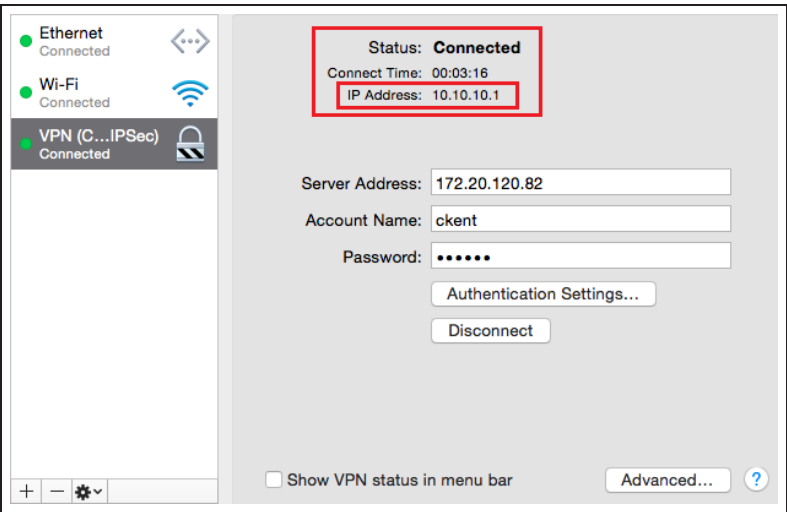
Group Name:

Cancel OK

## 4. Results

On the Mac, ensure that the VPN is selected and click **Connect**. The **Status** should change to **Connected** and you should be given an **IP Address** in the range specified **above**.

You should also be able to browse the Internet, protected by whichever profiles you applied to the security policy created in **the above step**.

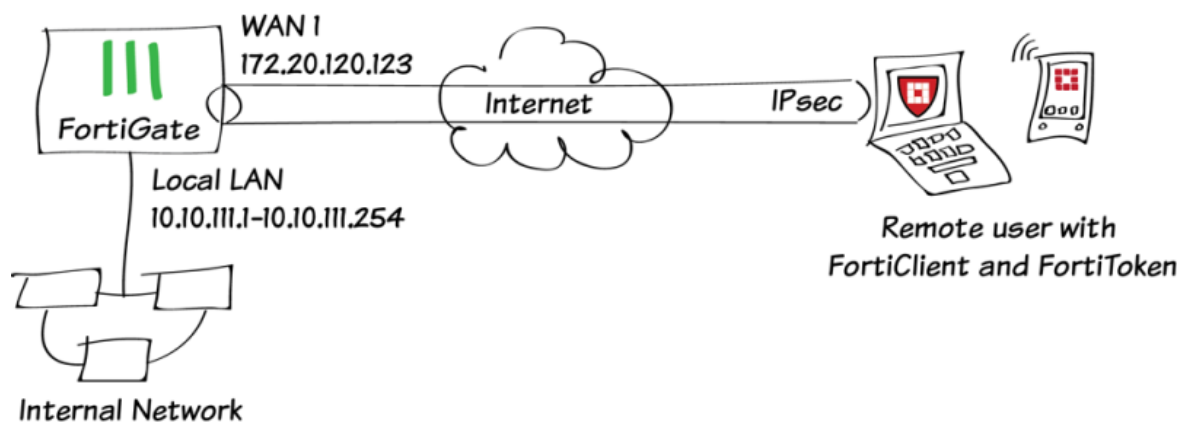


On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**, and that there are **Incoming** and **Outgoing Data**.

| Name        | Type                    | Remote Gateway | Username | Status | Incoming Data | Outgoing |
|-------------|-------------------------|----------------|----------|--------|---------------|----------|
| NativeMac_0 | Dialup - Cisco Firewall | 172.20.120.221 |          | Up     | 862.49 KB     | 2.06 MB  |

For further reading, check out **IPsec VPN** in **the web-based manager** in the **FortiOS 5.2 Handbook**.

# IPsec VPN with two-factor authentication



In this recipe, two-factor authentication is added to a user account to provide extra security when connecting to an IPsec VPN using FortiClient for Mac OS x.

Two-factor authentication requires a user to authenticate twice before being allowed to access the IPsec VPN. In this recipe the FortiToken Mobile app for iOS provides a one-time password (OTP) (a 6-digit number) that the you must enter at a second authentication prompt.

This recipe assumes that you have already activated FortiToken Mobile (see [Two-factor authentication with FortiToken Mobile](#) for details).

## 1. Creating a user and user group

Go to **User & Device > User > User Definition** and create a new local user.

The screenshot shows the 'User Type' step of the wizard. At the top, there are four steps: 1 User Type (active), 2 Login Credentials, 3 Contact Info, and 4 Extra Info. Below the steps, there are four radio button options: 'Local User' (selected), 'Remote RADIUS User', 'Remote TACACS+ User', and 'Remote LDAP User'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter the user's login credentials. This example simply creates a local user.

The screenshot shows the 'Login Credentials' step of the wizard. The steps at the top are: 1 User Type, 2 Login Credentials (active), 3 Contact Info, and 4 Extra Info. Below the steps, there are two text input fields: 'User Name' with the value 'jsimmons' and 'Password' with masked characters '.....'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

For **Contact Info**, select SMS and be sure to include a **Phone Number** without dashes or spaces.

This example uses SMS to send an activation code to the user so we included the user's mobile phone number here. Even if your FortiGate cannot send SMS messages you need to include a phone number for the IPsec VPN wizard to work.

Do *not* add an email address.

The screenshot shows the 'Contact Info' step of the wizard. The steps at the top are: 1 User Type, 2 Login Credentials, 3 Contact Info (active), and 4 Extra Info. Below the steps, there are four fields: 'Email Address' (empty), 'SMS' (checked checkbox), 'Country/Region' (dropdown menu showing 'United States/Canada'), 'Phone Number' (text input with '+1 5555555555'), and 'Service Type' (dropdown menu showing 'FortiGuard Messaging Service'). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.



Select the FortiToken assigned to this user.

User Type

Login Credentials

Contact Info

4 Extra Info

☒ Enable

☒ Two-factor Authentication

Token

FTKMOB37E71E8FFC

☐ User Group

Click to add...

< Back

Create

Cancel

The user list shows the FortiToken in the **Two-factor Authentication** column for the new user account.

| User Name | Type  | Two-factor Authentication |
|-----------|-------|---------------------------|
| guest     | LOCAL |                           |
| jsimmons  | LOCAL | FTKMOB37E71E8FFC          |

Go to **User & Device > User > User Groups**. Create a user group for remote users and add the new user.

Name

IPsecVPN

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

jsimmons

## 2. Adding a firewall address for the LAN

Go to **Policy & Objects > Objects > Addresses**.

Create a firewall address for your LAN's subnet.

Name

LAN

Type

IP/Netmask

Subnet / IP Range

192.168.150.0/255.255.255.0

Interface

lan (VLAN ID: 0)

Show in Address List

☒

Comments

0/255

### 3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)**.

*The tunnel name may not have any spaces.*

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Client Options

Name: OfficeVPN

Template:

- ☒ Dialup - FortiClient (Windows, Mac OS, Android)
- ☐ Site to Site - FortiGate
- ☐ Dialup - iOS (Native)
- ☐ Dialup - Android (Native L2TP/IPsec)
- ☐ Dialup - Cisco Firewall
- ☐ Site to Site - Cisco
- ☐ Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**. Enter a pre-shared key and select the new user group.

*The pre-shared key is a credential for the VPN and should differ from the user's password.*

OfficeVPN : Dialup - FortiClient (Windows, Mac OS, Android)

Incoming Interface: wan1

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key: ..... \*

☒ Hide Characters

User Group: IPsecVPN

< Back Next > Cancel

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the \_range suffix (in this case, ipsecvpn\_range).*

*In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.*

Select **Client Options** as desired.

VPN Setup

Authentication

3 Policy & Routing

4 Client Options

OfficeVPN : Dialup - FortiClient (Windows, Mac OS, Android)

Local Interface

lan (VLAN ID: 0)

Local Address

LAN

Client Address Range

10.10.13.1-10.10.13.254

Subnet Mask

255.255.255.255

DNS Server

☒ Use System DNS

☐ Specify

☐ Enable IPv4 Split Tunnel

☒ Allow Endpoint Registration

< Back

Next >

Cancel

VPN Setup

Authentication

Policy & Routing

4 Client Options

OfficeVPN : Dialup - FortiClient (Windows, Mac OS, Android)

☒ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

< Back

Create

Cancel

## 4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**. Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**. Set the **Source User(s)** to the new user group. Set **Outgoing Interface** to your Internet-facing interface and **Destination Address** to **all**.

Ensure that you enable **NAT**.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | OfficeVPN       |
| Source Address      | all             |
| Source User(s)      | IPsecVPN        |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address | all             |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 5. Sending the FortiToken activation code to the user

If your FortiGate can send SMS messages, go to **User & Device > User > User Definition** and edit the new user account. Select **Send Activation Code** and send the code by **SMS**.

**Send Activation Code**

Token: FTKMOB37E71E8FFC

Send Activation Code

☐ Email ☒ SMS

Warning: The activation code will be sent to the last saved SMS server configuration and number (15555555555)

OK Cancel

If your FortiGate cannot send SMS messages, go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct serial number:

```
config user fortitoken
edit
show
```

The activation code will be shown in the output. This code must be given to the user.

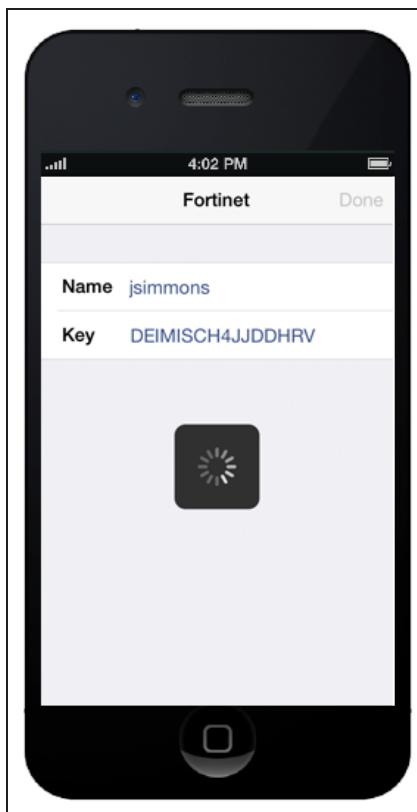
```
set activation-code "DEIMISCH4JJDDHRV"
```

## 6. Setting up FortiToken Mobile on an iOS device

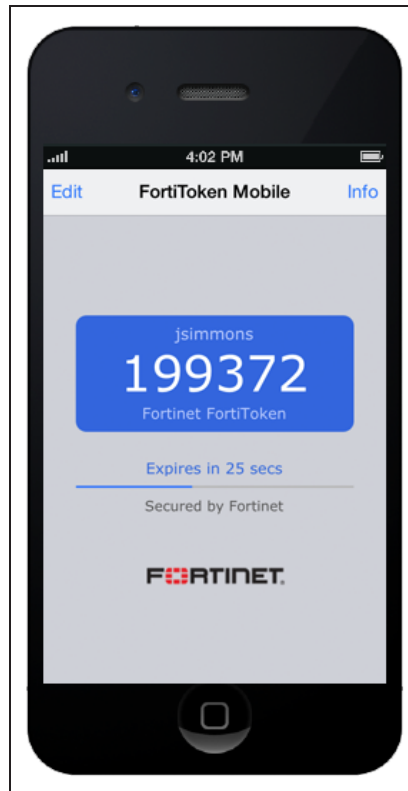
Using your iOS device, download and install **FortiToken Mobile**.

Open the app and add a new account. Select **Enter Manually**, then select **Fortinet** under **FORTINET ACCT**.

Enter the activation code into FortiToken Mobile.



FortiToken Mobile can now generate a token for use with the FortiGate.

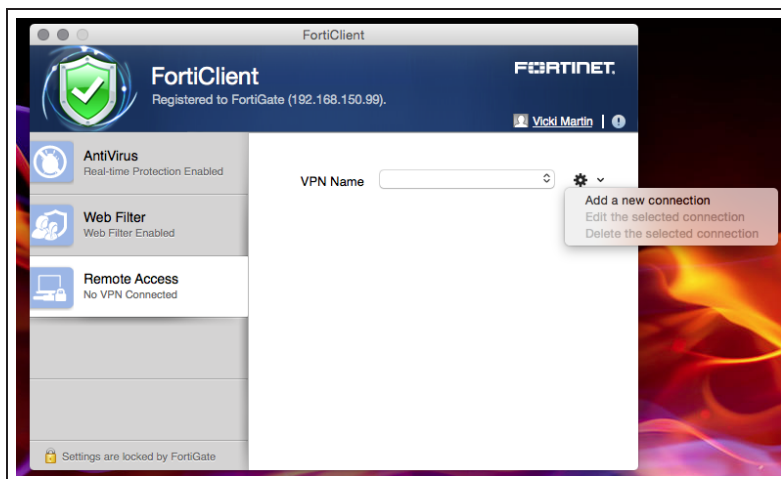


(Optional) For additional security, set a **PIN** for FortiToken Mobile using the app's **Settings** options.

## 7. Configuring FortiClient for Mac OS X

Using your Mac OS X device, download and install **FortiClient**.

Open FortiClient, go to **Remote Access** and select **Add a new connection**.



Provide a **Connection Name** and set the **Type** to IPsec VPN.

Set **Remote Gateway** to the FortiGate's IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key for the IPsec VPN.

|                               |  |
|-------------------------------|--|
| <b>VPN Type</b>               | <input type="radio"/> SSL VPN <input checked="" type="radio"/> IPsec VPN |
| <b>Connection Name</b>        | <input type="text" value="OfficeVPN"/>                                   |
| <b>Description</b>            | <input type="text" value="Description or Comment"/>                      |
| <b>Remote Gateway</b>         | <input type="text" value="172.20.120.41"/>                               |
| <b>Authentication Method</b>  | <input type="text" value="Pre-Shared Key"/>                              |
| <b>Pre-Shared Key</b>         | <input type="password" value="....."/>                                   |
| <b>Authentication (XAuth)</b> | <input checked="" type="checkbox"/> Save Login                           |
| <b>Username</b>               | <input type="text" value="jsimmons"/>                                    |

# 8. Results

Using FortiClient, select the IPsec VPN connection, enter the password, and click **Connect**.

VPN Name

OfficeVPN

Username

jsimmons

Password

.....

Connect

You will be prompted to enter your code from FortiToken mobile.

Connecting...

VPN Name

OfficeVPN

Username

jsimmons

Password

.....


Answer

.....|

FortiToken Code



After your code has been verified, a connection to the IPsec VPN is established.




OfficeVPN


10.10.13.1

jsimmons


---

 Duration

00:00:25

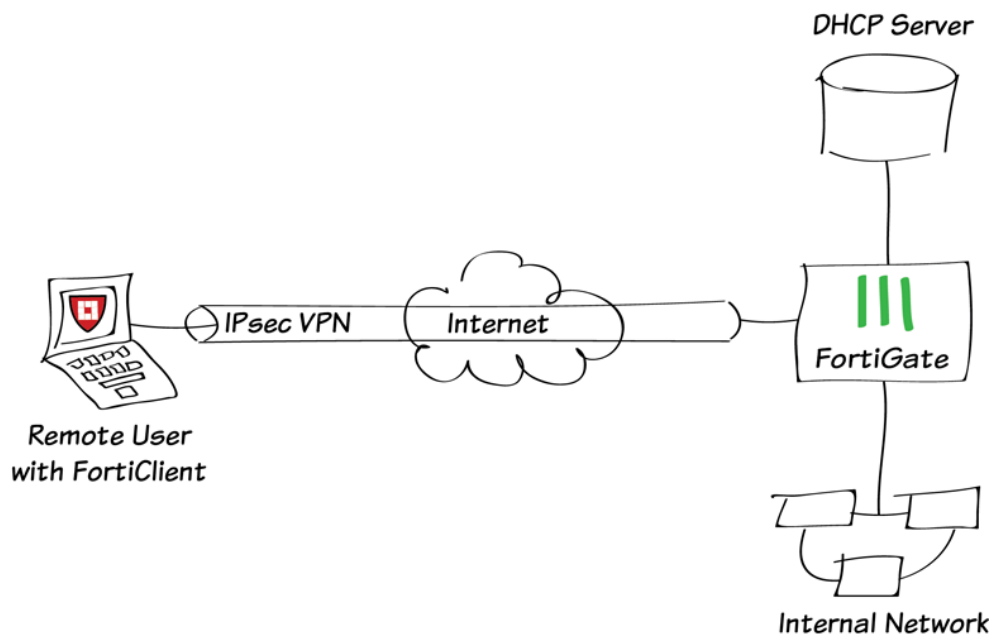
 Bytes Received

0

 Bytes Sent

432

# IPsec VPN with external DHCP service



In this recipe you'll use an external DHCP server to assign IP addresses to your IPsec VPN clients, this scenario is commonly found on enterprises where all DHCP leases need to be centrally managed.

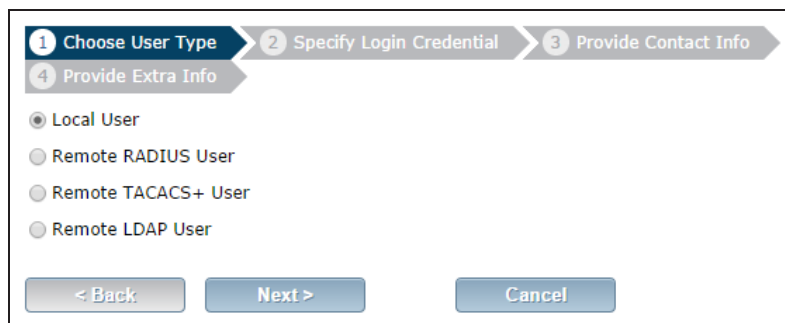
The DHCP server assigns IP addresses in the range of 172.16.6.100 to 172.16.6.120. The server is attached to port 4 of the FortiGate and has an IP address of 192.168.3.70.

## 1. Creating a user group for remote users

Go to **User & Device > User > User Definition**.

Create a new **Local User** with the **User Creation Wizard**.

Proceed through each step of the wizard, carefully entering the appropriate information.



The screenshot shows the first step of the User Creation Wizard. At the top, there are four numbered steps: 1. Choose User Type (active), 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info. Below the steps, there are four radio button options: Local User (selected), Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. At the bottom, there are three buttons: < Back, Next >, and Cancel.

Go to **User & Device > User > User Groups**.

Create a user group for remote users and add the user you created.

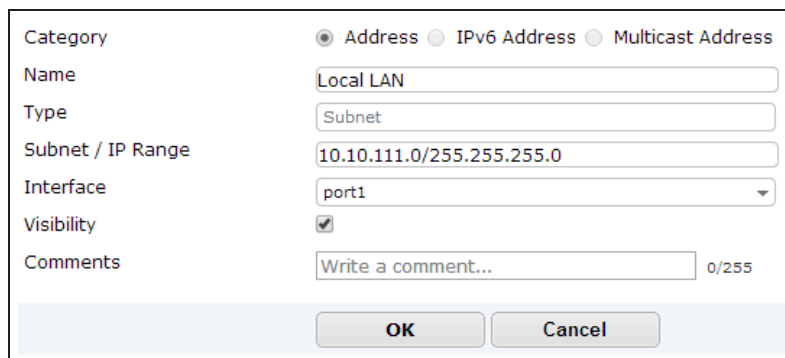


The screenshot shows the User Groups configuration form. The Name field is set to 'ipsecvpn'. The Type field has four radio button options: Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO). The Members field contains 'twhite' with a search icon and a plus icon. Below the Members field is a section for Remote groups with a table. The table has two columns: Remote Server and Group Name. The table is currently empty, showing 'No matching entries found'. At the bottom, there are OK and Cancel buttons.

## 2. Adding a firewall address for the local network and IPsec VPN client range

Go to **Policy & Objects > Objects > Addresses**.

Add a firewall address for the Local LAN, including the subnet and local interface.



The screenshot shows the Addresses configuration form. The Category field has three radio button options: Address (selected), IPv6 Address, and Multicast Address. The Name field is set to 'Local LAN'. The Type field is set to 'Subnet'. The Subnet / IP Range field is set to '10.10.111.0/255.255.255.0'. The Interface field is set to 'port1'. The Visibility field is checked. The Comments field is set to 'Write a comment...'. At the bottom, there are OK and Cancel buttons.

Add a firewall address for the IPsec VPN client range.

|                      |  |
|----------------------|--|
| Name                 | <input type="text" value="ipsecvpn_range"/>            |
| Type                 | <input type="text" value="IP Range"/>                  |
| Subnet / IP Range    | <input type="text" value="172.16.6.100-172.16.6.120"/> |
| Interface            | <input type="text" value="any"/>                       |
| Show in Address List | <input checked="" type="checkbox"/>                    |
| Comments             | <input type="text" value=""/> 0/255                    |

### 3. Configuring the IPsec VPN using a Custom VPN Tunnel

Go to **VPN > IPSec > Tunnels > Create New**.

Name the VPN connection and select **Custom VPN Tunnel (No Template)** and click Next.

*The tunnel name may not have any spaces in it.*

1 VPN Setup

Name

Template

Dialup - FortiClient (Windows, Mac OS, Android)

Site to Site - FortiGate

Dialup - iOS (Native)

Dialup - Android (Native L2TP/IPsec)

Dialup - Cisco Firewall

Site to Site - Cisco

Custom VPN Tunnel (No Template)

< Back

Next >

Cancel

Configure the following parameters:

Set the **Remote Gateway** to **Dialup User**

Set the **Interface** to the internet-facing interface.

Enter a **Pre-shared Key**.

*The pre-shared key is a credential for the VPN and should differ from the user's password.*

Set the **Mode** to **Aggressive**

Set the **XAUTH Type** to **Auto Server**

Set the **XAUTH User Group** to the User Group created on step 1 and click OK to apply the configuration

Use the CLI to enable DHCP-IPsec inside the VPN Phase 2 settings.

Name

dhcp\_vpn

Comments

Comments

Network

Remote Gateway : Dialup User , Interface : port6

Authentication

Authentication Method : Pre-shared Key  
IKE Version : 1 , Mode : Aggressive

Phase 1 Proposal

Algorithms : AES128-SHA256, AES256-SHA256, 3DES-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA1  
Diffie-Hellman Groups : 14, 5

XAUTH

Type : Auto Server , User Group : ipsecvpn

Phase 2 Selectors

| Name     | Local Address   | Remote Address  |                            |
|----------|-----------------|-----------------|----------------------------|
| dhcp_vpn | 0.0.0.0/0.0.0.0 | 0.0.0.0/0.0.0.0 | <div><div>+</div>Add</div> |

```
config vpn ipsec phase2-interface
edit "dhcp_vpn"
set dhcp-ipsec enable
next
end
```

## 4. Configuring the IPsec VPN Interface

Go to **System > Network > Interfaces**.

Edit the newly created IPsec VPN Interface

Set the **IP** to the same subnet that will be leased to VPN clients. This is the value that the DHCP Administrator must use for the DHCP Option 003 (Router). Set the **Remote IP** to the same value.

Enable **DHCP Server**, then expand **Advanced** and change the mode to **Relay**. Enter the external **DHCP server IP** address and change the **Type** to **IPsec**.

|  |  |  |  |  |  |
|--|--|--|--|--|--|
| Interface Name   | dhcp_vpn                                 |  |  |  |  |
| Type   | Tunnel Interface                         |  |  |  |  |
| Interface  | port6                                    |  |  |  |  |
| Addressing mode  |  |  |  |  |  |
| Manual   |  |  |  |  |  |
| IP   | <input type="text" value="172.16.6.10"/> |  |  |  |  |
| Remote IP  | <input type="text" value="172.16.6.10"/> |  |  |  |  |
| Administrative Access  |  |  |  |  |  |
| <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP |  |  |  |  |  |
| <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access   |  |  |  |  |  |
| DHCP Server  |  |  |  |  |  |
| <input checked="" type="checkbox"/> Enable   |  |  |  |  |  |
| ▼ Advanced...  |  |  |  |  |  |
| Mode   |  |  |  |  |  |
| <input type="radio"/> Server <input checked="" type="radio"/> Relay  |  |  |  |  |  |
| DHCP Server IP   |  |  |  |  |  |
| <input type="text" value="192.168.3.70"/>  |  |  |  |  |  |
| Type   |  |  |  |  |  |
| <input type="radio"/> Regular <input checked="" type="radio"/> IPsec   |  |  |  |  |  |

## 5. Creating a security policy for access to the Local LAN Network

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing the VPN IPsec client IP address range to access the Local LAN network.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to the VPN IPsec client range defined on step 2.

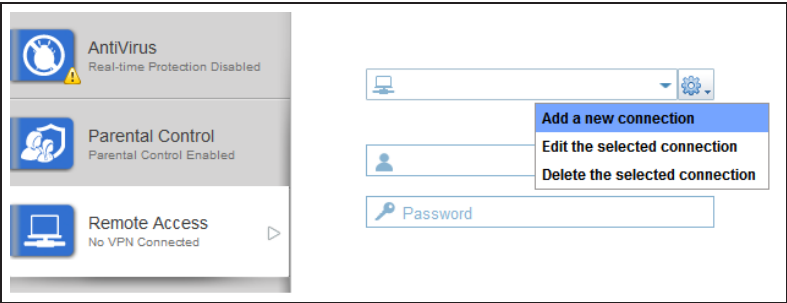
Set **Outgoing Interface** to **port4** and **Destination Address** to **Local LAN**.

Set **Service** to **ALL**

|                                   |  |   |
|-----------------------------------|--|---|
| Incoming Interface                | <input type="text" value="dhcp_vpn"/>        | + |
| Source Address                    | <input type="text" value="ipsecvpn_range"/>  | + |
| Source User(s)                    | <input type="text" value="Click to add..."/> |   |
| Source Device Type                | <input type="text" value="Click to add..."/> |   |
| Outgoing Interface                | <input type="text" value="port4 (lan)"/>     | + |
| Destination Address               | <input type="text" value="Local LAN"/>       | + |
| Schedule                          | <input type="text" value="always"/>          |   |
| Service                           | <input type="text" value="ALL"/>             | + |
| Action                            | <input type="text" value="ACCEPT"/>          |   |
| <b>Firewall / Network Options</b> |  |   |
| <input type="checkbox"/> OFF NAT  |  |   |

## 6. Configuring FortiClient

Open FortiClient, go to **Remote Access** and **Add a new connection**.



Provide a **Connection Name** and set the **Type** to IPsec VPN.

Set **Remote Gateway** to the FortiGate external IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key below.


|                        |  |
|------------------------|--|
| Connection Name        | IPsec VPN to Work  |
| Type                   | <input type="radio"/> SSL-VPN <input checked="" type="radio"/> IPsec VPN             |
| Description            |  |
| Remote Gateway         | 172.20.120.123   |
| Authentication Method  | Pre-Shared Key   |
| Pre-Shared Key         | ••••••   |
| Authentication (XAuth) | <input checked="" type="radio"/> Prompt on login<br><input type="radio"/> Save login |


Expand **Advanced Settings** and **VPN Settings**.


Select **DHCP over IPsec**.

|                            |   |
|----------------------------|---|
| ▼ <b>Advanced Settings</b> |   |
| ▼ <b>VPN Settings</b>      |   |
| Mode                       | <input type="radio"/> Main <input checked="" type="radio"/> Aggressive  |
| Options                    | <input type="radio"/> Mode Config <input type="radio"/> Manually Set <input checked="" type="radio"/> DHCP over IPsec |

Select the new connection, enter the username and password, and click **Connect**.

 **Antivirus**  
Real-time Protection Disabled

 **Parental Control**  
Parental Control Enabled

 **Remote Access**  
No VPN Connected

IPsec VPN to Work


white


•••••


Connect


7. Results

Once the connection is established, the external DHCP server assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.

 **Antivirus**  
Real-time Protection Disabled

 **Parental Control**  
Parental Control Enabled

 **Remote Access**  
VPN Connected

 **IPsec VPN to Work**  
10.10.111.16

Duration00:00:23

Bytes Received8344

Bytes Sent157192

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

| Name    | Ty...  | Remote Gatew... | Stat... | Incoming D... | Outgoing Data |
|---------|--------|-----------------|---------|---------------|---------------|
| ipsec_0 | Dialup | 172.20.120.16   | Up      | 9.22 K        | 3.48 K        |

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

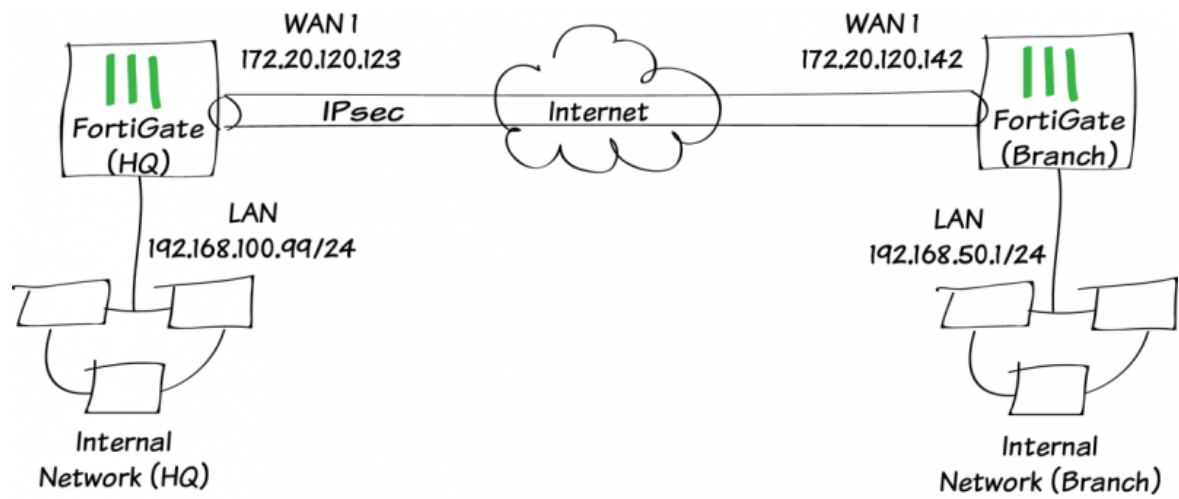
Verify that the **Sent/Received** column displays traffic successfully flowing through the tunnel.

| # | Date/Time | Src Interface | Dst Interface | Src          | Dst           | Sent / Received |
|---|-----------|---------------|---------------|--------------|---------------|-----------------|
| 1 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 59 B / 221 B    |
| 2 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 60 B / 292 B    |
| 3 | 11:22:41  | ipsecvpn      | wan1          | 10.10.111.16 | 208.91.112.53 | 56 B / 288 B    |



For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

# Site-to-site IPsec VPN with two FortiGates



In this example, you will allow transparent communication between two networks that are located behind different FortiGates at different offices using route-based IPsec VPN. The VPN will be created on both FortiGates by using the VPN Wizard’s **Site to Site FortiGate** template.

In this example, one office will be referred to as HQ and the other will be referred to as Branch.

A video of this recipe is available [here](#).

## 1. Configuring the HQ IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name

Template

- ☐ Dialup - FortiClient (Windows, Mac OS, Android)
- ☒ Site to Site - FortiGate
- ☐ Dialup - IOS (Native)
- ☐ Dialup - Android (Native L2TP/IPsec)
- ☐ Dialup - Cisco Firewall
- ☐ Site to Site - Cisco
- ☐ Custom VPN Tunnel (No Template)

< Back Next > Cancel

In the **Authentication** step, set the Branch FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.142*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

Set a secure **Pre-shared Key**

1 VPN Setup 2 Authentication 3 Policy & Routing

HQ-to-Branch : Site to Site - FortiGate

Remote Gateway

Outgoing Interface wan1 ( Detected via routing lookup ) [\[Change\]](#)

Authentication Method ☒ Pre-shared Key ☐ Signature

Pre-shared Key

☒ Hide Characters

< Back Next > Cancel

In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the Branch FortiGate's local subnet (in the example, *192.168.50.0/24*).

VPN Setup

Authentication

3 Policy & Routing

HQ-to-Branch : Site to Site - FortiGate

Local Interface

lan

Local Subnets

192.168.100.0/24

Remote Subnets

192.168.50.0/24

< Back

Create

Cancel

A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

✔The VPN has been set up

Summary of Created Objects

|                        |                     |
|------------------------|---------------------|
| Phase 1 Interface      | HQ-to-Branch        |
| Phase 2 Interfaces     | HQ-to-Branch        |
| Static Routes          | 192.168.50.0/24     |
| Local Address Group    | HQ-to-Branch_local  |
| Remote Address Group   | HQ-to-Branch_remote |
| Local to Remote Policy | 2                   |
| Remote to Local Policy | 3                   |

## 2. Configuring the Branch IPsec VPN

On the Branch FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name

Template

- ☐ Dialup - FortiClient (Windows, Mac OS, Android)
- ☒ Site to Site - FortiGate
- ☐ Dialup - IOS (Native)
- ☐ Dialup - Android (Native L2TP/IPsec)
- ☐ Dialup - Cisco Firewall
- ☐ Site to Site - Cisco
- ☐ Custom VPN Tunnel (No Template)

< Back Next > Cancel

In the **Authentication** step, set the HQ FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.123*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

Set the same **Pre-shared Key** that was used for HQ's VPN.

1 VPN Setup 2 Authentication 3 Policy & Routing

Branch-to-HQ : Site to Site - FortiGate

Remote Gateway

Outgoing Interface wan1 ( Detected via routing lookup ) [\[Change\]](#)

Authentication Method ☒ Pre-shared Key ☐ Signature

Pre-shared Key

☒ Hide Characters

< Back Next > Cancel

In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the HQ FortiGate's local subnet (in the example, *192.168.100.0/24*).

VPN Setup

Authentication

3 Policy & Routing

Branch-to-HQ : Site to Site - FortiGate

Local Interface

lan

Local Subnets

192.168.50.0/24

Remote Subnets

192.168.100.0/24

< Back

Create

Cancel

A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

✔ The VPN has been set up

Summary of Created Objects

|                        |                     |
|------------------------|---------------------|
| Phase 1 Interface      | Branch-to-HQ        |
| Phase 2 Interfaces     | Branch-to-HQ        |
| Static Routes          | 192.168.100.0/24    |
| Local Address Group    | Branch-to-HQ_local  |
| Remote Address Group   | Branch-to-HQ_remote |
| Local to Remote Policy | 1                   |
| Remote to Local Policy | 2                   |

### 3. Results

A user on either of the office networks should be able to connect to any address on the other office network transparently.

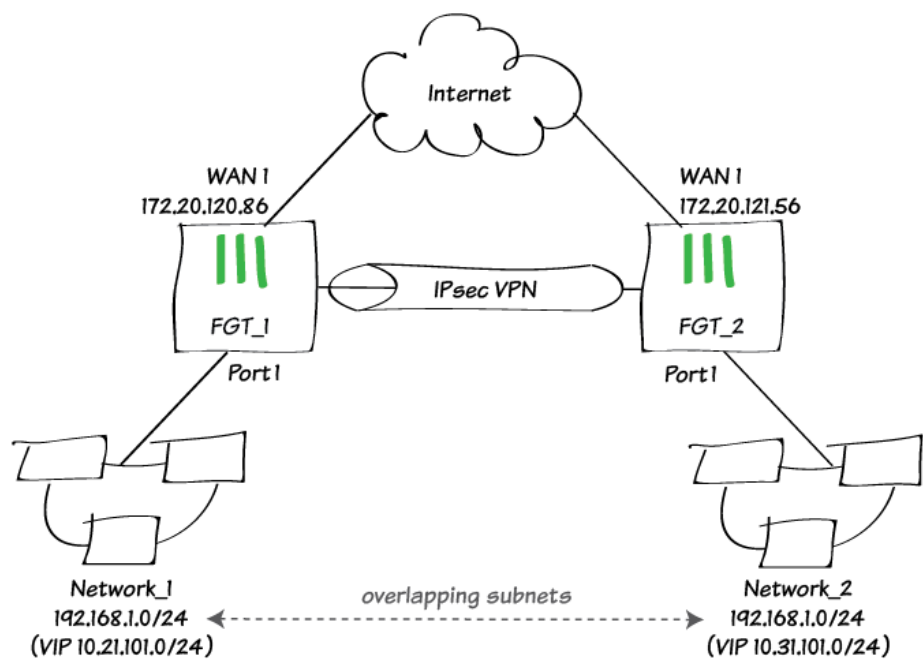
If you need to generate traffic to test the connection, ping the Branch FortiGate's internal interface from the HQ's internal network.

Go to **VPN > Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Ensure that its **Status** is **Up** and that traffic is flowing.

| Name         | Type   | Remote Gateway | Status   | Incoming Data | Outgoing Data |
|--------------|--|----------------|--|---------------|---------------|
| Branch-to-HQ |  Site to Site - FortiGate | 172.20.120.236 |  Up | 1.63 KB       | 1.56 KB       |

For further reading, check out [Gateway-to-gateway configurations](#) in the [FortiOS 5.2 Handbook](#).

# Site-to-site IPsec VPN with overlapping subnets



This recipe describes how to construct a site-to-site IPsec VPN connection between two networks with overlapping subnets, such that traffic will be directed to the correct address on the correct network, using Virtual IP addresses and static routes.

A video of this recipe is available [here](#).



## 1. Create the IPsec VPN tunnel on FGT\_1

Go to **VPN > IPsec > Wizard**.

Select **Site to Site - FortiGate**. Give it an appropriate **Name** and click **Next**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name Site to Site

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set **Remote Gateway** to the IP address used by the Internet-facing interface of FGT\_2. The Outgoing Interface will automatically populate.

Enter a **Pre-shared key** and click **Next**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Site to Sites : Site to Site - FortiGate

Remote Gateway 172.20.120.86

Outgoing Interface wan1 ( Detected via routing lookup ) [Change]

Authentication Method ☒ Pre-shared Key ☐ Signature

Pre-shared Key .....

☒ Hide Characters

< Back Next > Cancel

Set **Local Interface** to your Internet-facing interface. The **Local Subnets** will automatically populate. Set **Remote Subnets** to the VIP of the internal network for FGT\_2 (10.31.101.0/24) and click **Create**.

VPN Setup

Authentication

3 Policy & Routing

Site to Sites : Site to Site - FortiGate

Local Interface

port1

Local Subnets

192.168.1.0/24

Remote Subnets

10.31.101.0/24

< Back

Create

Cancel

The VPN Wizard automatically creates the required objects, policies, and static route required for the tunnel to function properly.

VPN Setup

Authentication

Policy & Routing

Site to Site : Site to Site - FortiGate

The VPN has been set up

Summary of Created Objects

Phase 1 Interface

Site to Site

Phase 2 Interfaces

Site to Site

Static Routes

10.31.101.0/24

Local Address Group

Site to Site\_local

Remote Address Group

Site to Site\_remote

Local to Remote Policy

4

Remote to Local Policy

5

Add Another

Show Tunnel List

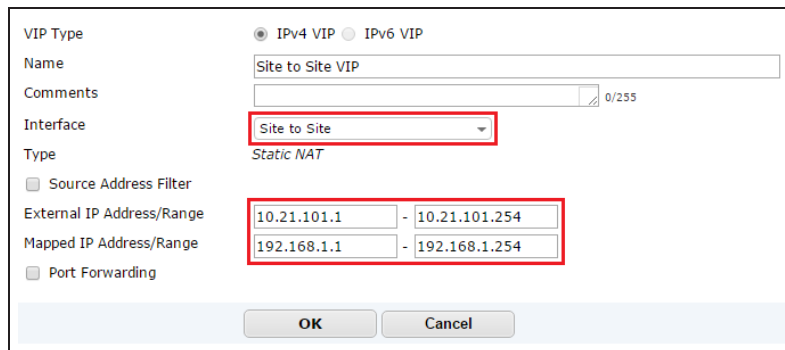
You can verify the policy creation under **Policy & Objects > Policy > IPv4**.

| Seq.# | From             | To           | Source              | Destination         | Schedule | Service | Action |
|-------|------------------|--------------|---------------------|---------------------|----------|---------|--------|
| 1     | port1 (Internal) | wan1         | all                 | all                 | always   | ALL     | ACCEPT |
| 2     | port2            | wan1         | all                 | all                 | always   | ALL     | ACCEPT |
| 3     | WiFi (SSID)      | wan1         | all                 | all                 | always   | ALL     | ACCEPT |
| 4     | wan1             | Site to Site | Site to Site_local  | Site to Site_remote | always   | ALL     | ACCEPT |
| 5     | Site to Site     | wan1         | Site to Site_remote | Site to Site_local  | always   | ALL     | ACCEPT |
| 6     | any              | any          | all                 | all                 | always   | ALL     | DENY   |

## 2. Add the Virtual IP Range on FGT\_1

Go to **Policy & Objects > Objects > Virtual IPs** and create a Virtual IP range to redirect the traffic to the correct subnet.

Select **Virtual IP** from the **Create New** drop down menu. Select **IPv4** for the **VIP Type** and give the VIP an appropriate name.



VIP Type: ☒ IPv4 VIP ☐ IPv6 VIP

Name: Site to Site VIP

Comments: 0/255

Interface: Site to Site

Type: Static NAT

☐ Source Address Filter

External IP Address/Range: 10.21.101.1 - 10.21.101.254

Mapped IP Address/Range: 192.168.1.1 - 192.168.1.254

☐ Port Forwarding

OK Cancel

Set the **Interface** to the IPsec VPN **Site to Site** interface from the drop down menu.


Set **External IP Address/Range** to a range in the subnet you will be redirecting from (10.21.101.1 - 10.21.101.254) and **Mapped IP Address/Range** to the internal network range (192.168.1.1 - 192.168.1.254).

Select **OK**.

## 3. Create the IPsec VPN tunnel on FGT\_2

Go to **VPN > IPsec > Wizard**.

Select **Site to Site - FortiGate**. Give it an appropriate **Name** and click **Next**.



1 VPN Setup 2 Authentication 3 Policy & Routing

Name: Site to Site

Template:

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set **Remote Gateway** to the IP address used by the Internet-facing interface of FGT\_1. The Outgoing Interface will automatically populate.

Enter a **Pre-shared key** and click **Next**.

VPN Setup

2 Authentication

3 Policy & Routing

Site to Sites : Site to Site - FortiGate

Remote Gateway

172.20.121.56

Outgoing Interface

wan1 ( Detected via routing lookup ) [Change]

Authentication Method

Pre-shared Key

Signature

Pre-shared Key

Hide Characters

< Back

Next >

Cancel

Set **Local Interface** to your Internet-facing interface. The **Local Subnets** will automatically populate. Set **Remote Subnets** to the VIP of the internal network for FGT\_1 (10.21.101.0/24) and click **Create**.

VPN Setup

Authentication

3 Policy & Routing

Site to Sites : Site to Site - FortiGate

Local Interface

port1

Local Subnets

192.168.1.0/24

Remote Subnets

10.21.101.0/24

< Back

Create

Cancel

The VPN Wizard automatically creates the required objects, policies, and static route required for the tunnel to function properly.

As before, you can verify the policy creation under **Policy & Objects > Policy > IPv4**.

VPN Setup

Authentication

Policy & Routing

Site to Site : Site to Site - FortiGate

The VPN has been set up

Summary of Created Objects

|                        |                     |
|------------------------|---------------------|
| Phase 1 Interface      | Site to Site        |
| Phase 2 Interfaces     | Site to Site        |
| Static Routes          | 10.21.101.0/24      |
| Local Address Group    | Site to Site_local  |
| Remote Address Group   | Site to Site_remote |
| Local to Remote Policy | 4                   |
| Remote to Local Policy | 5                   |

Add AnotherShow Tunnel List

#### 4. Add the Virtual IP Range on FGT\_2

Go to **Policy & Objects > Objects > Virtual IPs** and create a Virtual IP range to redirect the traffic to the correct subnet.

Select **Virtual IP** from the **Create New** drop down menu. Select **IPv4** for the **VIP Type** and give the VIP an appropriate name.

VIP Type

☒ IPv4 VIP☐ IPv6 VIP

Name

Site to Site VIP

Comments

Interface

Site to Site

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

10.31.101.1 - 10.31.101.254

Mapped IP Address/Range

192.168.1.1 - 192.168.1.254

☐ Port Forwarding

OK

Cancel

Set **Interface** to the IPsec VPN **Site to Site** interface from the drop down menu.

Set **External IP Address/Range** to a range in the subnet you will be redirecting from (10.31.101.1 - 10.31.101.254) and **Mapped IP Address/Range** to the internal network range (192.168.1.1 - 192.168.1.254).

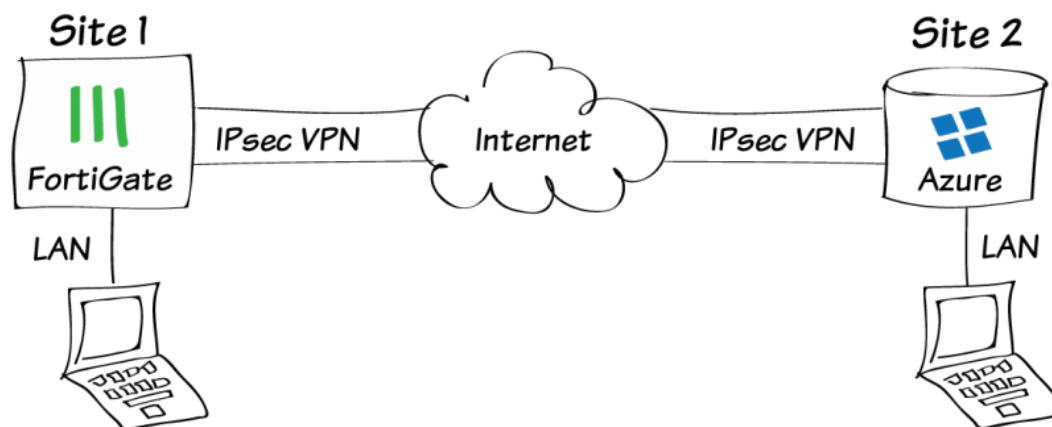
Select **OK**.

#### 5. Results

You will be able to see **Incoming** and **Outgoing Data** in the IPsec Monitor.

| Name         | Type   | Remote Gateway | Username | Status   | Incoming Data | Outgoing Data |  |
|--------------|--|----------------|----------|--|---------------|---------------|--|
| Site to Site |  Site to Site - FortiGate | 172.20.121.56  |          |  Up | 760 B         | 420 B         |  |

# IPsec VPN to Microsoft Azure



The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is hosted on Microsoft Azure™, for which you will need a valid Microsoft Azure profile.

Using FortiOS 5.2, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied.

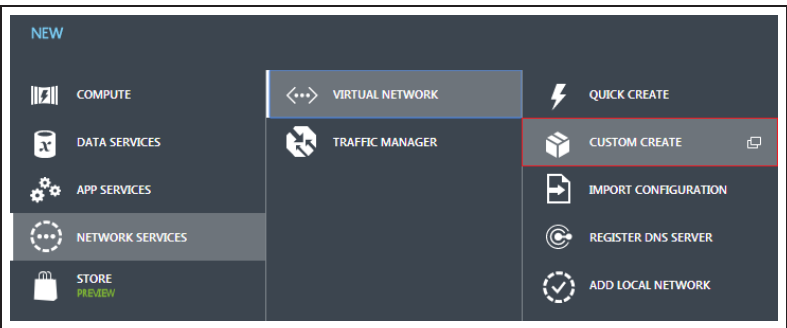
A video of this recipe is available [here](#).

# 1. Configuring the Microsoft Azure™ virtual network

Log into Microsoft Azure and click New in the lower-left corner to add a new service.



From the prompt, select **Network Services > Virtual Network > Custom Create**.



Under 'Virtual Network Details', enter a **Name** for the VPN and a **Location** where you want the VMs to reside, then click the **Next** arrow.

|   |                                      |
|---|--------------------------------------|
| NAME                                      | LOCATION                             |
| <input type="text" value="Site2SiteVPN"/> | <input type="text" value="East US"/> |

Under 'DNS Servers and VPN Connectivity', enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

|   |  |
|---|--|
| DNS SERVERS ?   | POINT-TO-SITE CONNECTIVITY ?                                     |
| <div><input type="text"/><input type="text"/></div> <div><input type="text" value="ENTER NAME"/><input type="text" value="IP ADDRESS"/></div> | <input type="checkbox"/> Configure a point-to-site VPN           |
|   | SITE-TO-SITE CONNECTIVITY ?                                      |
|   | <input checked="" type="checkbox"/> Configure a site-to-site VPN |
|   | <input type="checkbox"/> Use ExpressRoute                        |

Click the **Next** arrow.

Under 'Site-to-Site Connectivity', enter a **Name** and **IP Address** for the FortiGate device.

|  |  |               |                      |                                 |
|--|--|---------------|----------------------|---------------------------------|
| NAME                                       | ADDRESS SPACE                                    |               |                      |                                 |
| <input type="text" value="Local_Network"/> | ADDRESS SPACE                                    | STARTING IP   | CIDR (ADDRESS COUNT) | USABLE ADDRESS RANGE            |
| VPN DEVICE IP ADDRESS                      | 192.168.111.0/24                                 | 192.168.111.0 | /24 (256)            | 192.168.111.0 - 192.168.111.255 |
| <input type="text"/>                       | <input type="button" value="add address space"/> |               |                      |                                 |

Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

Click the **Next** arrow.



Under 'Virtual Network Address Spaces', configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the Checkmark in the lower-right corner to accept the configuration.

| ADDRESS SPACE | STARTING IP | CIDR (ADDRESS COUNT) | USABLE ADDRESS RANGE      |
|---------------|-------------|----------------------|---------------------------|
| 10.0.0.0/8    | 10.0.0.0    | /8 (16777...         | 10.0.0.4 - 10.255.255.254 |
| SUBNETS       |             |                      |                           |
| Subnet-1      | 10.11.12.0  | /24 (251)            | 10.11.12.4 - 10.11.12.254 |
| Gateway       | 10.11.13.0  | /29 (3)              | 10.11.13.4 - 10.11.13.6   |
| add subnet    |             | add gateway subnet   |                           |

After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn't be long.

1 OPERATION IS CURRENTLY RUNNING

Creating virtual network 'Site2SiteVPN'...

## 2. Creating the Microsoft Azure™ virtual network gateway

On the 'networks' home screen, click the name of the virtual network you just created.

| NAME           | STATUS    |
|----------------|-----------|
| Site2SiteVPN → | ✓ Created |

Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.

Site2SiteVPN

THE GATEWAY WAS NOT CREATED.

GATEWAY

VPN

Local Network

At the bottom of the screen, select **Create Gateway > Dynamic Routing**.  
When prompted, select **Yes**.

Static Routing

Dynamic Routing

+

↓

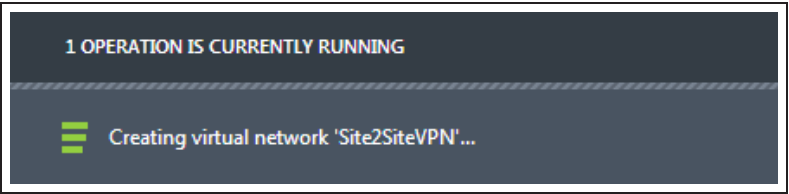
🗑

CREATE GATEWAY

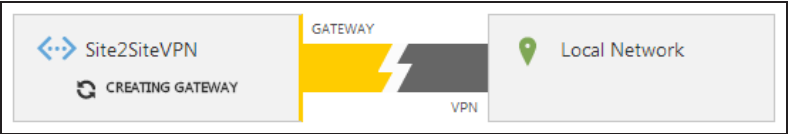
EXPORT

DELETE

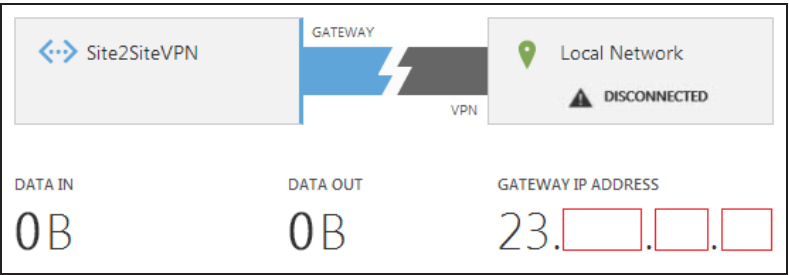
The operation to create the virtual network gateway will run. The process takes a short amount of time.



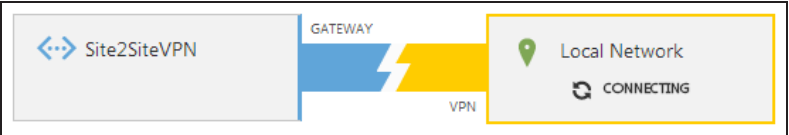
Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.



When the operation is complete, the status changes and you are given a **Gateway IP Address**.



The gateway will then attempt to connect to the Local Network.

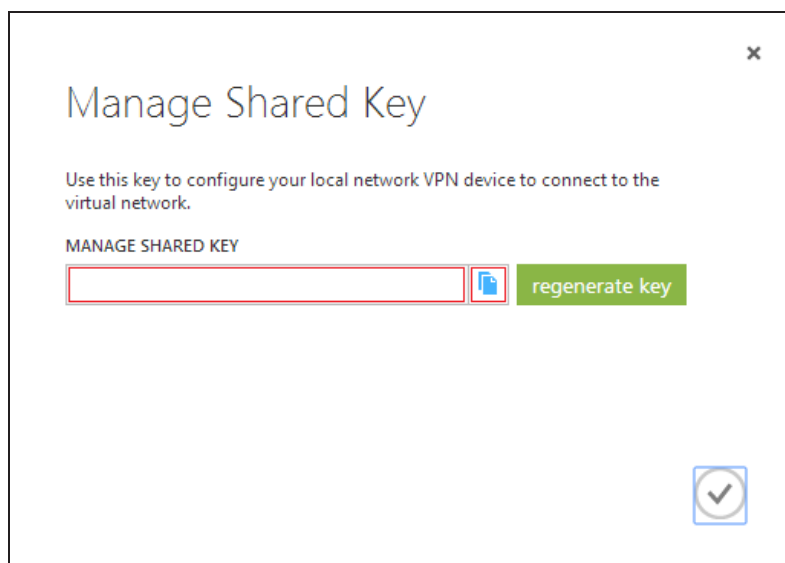


At the bottom of the screen, select **Manage Key**.



The 'Manage Shared Key' dialogue appears. **Copy** the key that is shown. You can select **regenerate key** if you want to copy a different key.

Click the **Checkmark** when you are confident that the key is copied.



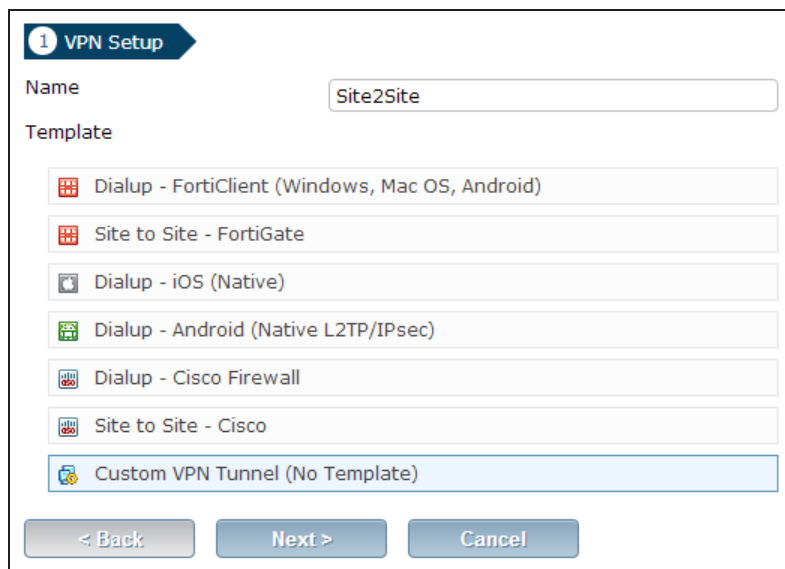
The 'Manage Shared Key' dialog box is shown. It has a title bar with a close button (X). The main text says 'Use this key to configure your local network VPN device to connect to the virtual network.' Below this, there is a section labeled 'MANAGE SHARED KEY' containing a text input field and a 'regenerate key' button. A checkmark icon is located in the bottom right corner of the dialog.

You are now ready to configure the FortiGate endpoint of the tunnel.

### 3. Configuring the FortiGate tunnel

Go to **VPN > IPsec > Wizard** and select **Custom VPN Tunnel (No Template)**.

Enter a **Name** for the tunnel and click **Next**.



The 'VPN Setup' wizard screen is shown. It has a title bar with a '1 VPN Setup' indicator. The 'Name' field is set to 'Site2Site'. The 'Template' list includes: 'Dialup - FortiClient (Windows, Mac OS, Android)', 'Site to Site - FortiGate', 'Dialup - iOS (Native)', 'Dialup - Android (Native L2TP/IPsec)', 'Dialup - Cisco Firewall', 'Site to Site - Cisco', and 'Custom VPN Tunnel (No Template)'. The 'Custom VPN Tunnel (No Template)' option is selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Transversal** and **Dead Peer Detection**.

Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56660** seconds.

NameSite2Site

CommentsComments

Enable IPsec Interface Mode☒

Network

IP Version

IPv4

IPv6

Remote Gateway

Static IP Address

IP Address

Local Interface

wan1

Mode Config☐

NAT Traversal☐

Dead Peer Detection☐

Authentication

Method

Pre-shared Key

Pre-shared Key

.....

Show Key

IKE

Version

1

2

Phase 1 Proposal

Encryption

AES256

Authentication

SHA1

Remove

Encryption

AES256

Authentication

SHA256

Remove

Encryption

AES128

Authentication

SHA1

Remove

Encryption

AES128

Authentication

SHA256

Remove

Diffie-Hellman Group

☐ 21

☐ 20

☐ 19

☐ 18

☐ 17

☐ 16

☐ 15

☐ 14

☐ 5

☒ 2

☐ 1

Key Lifetime (seconds)

56660

Local ID

VPNs

367

Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200 seconds**.

Phase 2 Selectors

| Name      | Local Address               | Remote Address           |
|-----------|-----------------------------|--------------------------|
| Site2Site | 192.168.111.0/255.255.255.0 | 10.11.12.0/255.255.255.0 |

Edit Phase 2

Name

Site2Site

Comments

VPN: Site2Site (Created by VPN wizard)

Local Address

Subnet192.168.111.0/255.255.255.0

Remote Address

Subnet10.11.12.0/255.255.255.0

Advanced...

Phase 2 Proposal

Encryption

AES128

Authentication

SHA256

Remove

Encryption

AES256

Authentication

SHA256

Remove

Encryption

AES128

Authentication

SHA1

Remove

Encryption

AES256

Authentication

SHA1

Remove

Enable Replay Detection

☒

Enable Perfect Forward Secrecy (PFS)

☐

Local Port

All

☒

Remote Port

All

☒

Protocol

All

☒

Autokey Keep Alive

☐

Auto-negotiate

☐

Key Lifetime

Seconds

7200

## 4. Creating the FortiGate firewall addresses

Go to **Policy & Objects > Objects > Addresses** and configure a firewall address for the local network.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | Internal_Port1  |
| Type                 | Subnet  |
| Subnet / IP Range    | 192.168.111.0/255.255.255.0   |
| Interface            | any   |
| Visibility           | <input checked="" type="checkbox"/>   |
| Comments             | <input type="text" value="Write a comment..."/> 0/255   |
| <div>OK Cancel</div> |   |

Create another firewall object for the Azure VPN tunnel subnet.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | AzureVPN-tunnel   |
| Type                 | Subnet  |
| Subnet / IP Range    | 10.11.12.0/255.255.255.0  |
| Interface            | any   |
| Visibility           | <input checked="" type="checkbox"/>   |
| Comments             | <input type="text" value="Write a comment..."/> 0/255   |
| <div>OK Cancel</div> |   |

## 5. Creating the FortiGate firewall policies

Go to **Policy & Objects > Policy > IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic

Set the **Source Address** and **Destination Address** using the firewall objects you just created.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | internal1       | + |
| Source Address      | Internal_Port1  | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | Site2Site       | + |
| Destination Address | AzureVPN-tunnel | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

When you are done, create another policy for the same connection to allow incoming traffic.

This time, invert the **Source Address** and **Destination Address**.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | Site2Site       |
| Source Address      | AzureVPN-tunnel |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | internal1       |
| Destination Address | Internal_Port1  |
| Schedule            | always          |
| Service             | ALL             |
| Action              | ACCEPT          |

6. Results

Go to **VPN > Monitor > IPsec > Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.

| Name      | Type                     | Remote Gateway | Username | Status |
|-----------|--------------------------|----------------|----------|--------|
| Site2Site | Static IP or Dynamic DNS |                |          | Down   |

Go to **Log & Report > Event Log > VPN**.

| Name      | Type                     | Remote Gateway | Username | Status |
|-----------|--------------------------|----------------|----------|--------|
| Site2Site | Static IP or Dynamic DNS |                |          | Up     |

Select an entry to view more information and verify the connection.

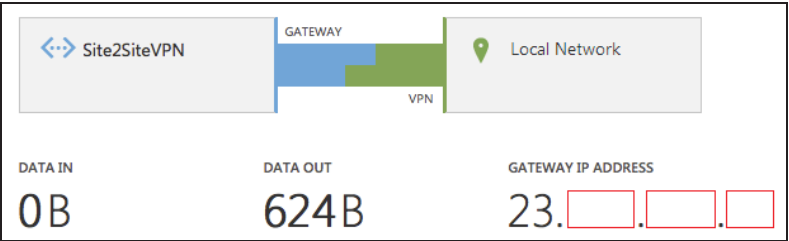
Go to **Log & Report > Event Log > VPN**.

Select an entry to view more information and verify the connection.

| #                         | Date/Time                         | Level | Action          | Status                  | Message                     | VPN Tunnel |
|---------------------------|-----------------------------------|-------|-----------------|-------------------------|-----------------------------|------------|
| 12                        | 15:23:04                          |       | phase2-up       |                         | IPsec phase 2 status change | Site2Site  |
| 13                        | 15:23:04                          |       | install_sa      |                         | install IPsec SA            | Site2Site  |
| 14                        | 15:23:04                          |       | negotiate       | success                 | negotiate IPsec phase 2     | Site2Site  |
| 15                        | 15:23:04                          |       | negotiate       | success                 | progress IPsec phase 1      | Site2Site  |
| 16                        | 15:23:04                          |       | negotiate       | success                 | negotiate IPsec phase 1     | Site2Site  |
| 1 / 1582 [ Total: 79053 ] |                                   |       |                 |                         |                             |            |
| Action                    | negotiate                         |       | Assigned IP     | N/A                     |                             |            |
| Cookies                   | 9de897c069896c80/31b2351571a476b2 |       | Date/Time       | 15:23:04 (1407770584)   |                             |            |
| ESP Authentication        | HMAC_SHA1                         |       | ESP Transform   | ESP_AES                 |                             |            |
| Group                     | N/A                               |       | IPsec Local IP  | 69.171.153.181          |                             |            |
| IPsec Remote IP           | 23.100.122.11                     |       | Level           | notice                  |                             |            |
| Local Port                | 500                               |       | Log Description | negotiate IPsec phase 2 |                             |            |
| Log ID                    | 37186                             |       | Message         | negotiate IPsec phase 2 |                             |            |
| Outgoing Interface        | ppp1                              |       | Remote Port     | 500                     |                             |            |
| Role                      | Initiator                         |       | Status          | success                 |                             |            |
| Sub Type                  | vpn                               |       | Timestamp       | 8/11/2014, 3:23:04 PM   |                             |            |
| User                      | N/A                               |       | VPN Tunnel      | Site2Site               |                             |            |
| Virtual Domain            | root                              |       | XAUTH Group     | N/A                     |                             |            |
| XAUTH User                | N/A                               |       |                 |                         |                             |            |

Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

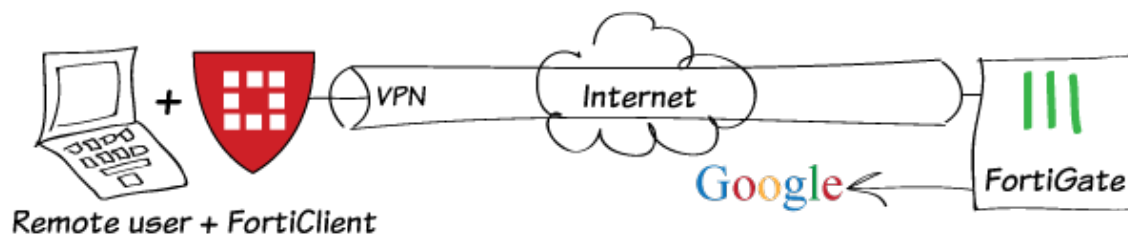
**Data In** and **Data Out** will indicate that traffic is flowing.



For further reading, check out [Gateway-to-gateway configurations](#) in the [FortiOS 5.2 Handbook](#).



# Remote Internet browsing using a VPN



In this recipe, you will use remote IPsec and SSL VPN tunnels to bypass Internet access restrictions.

Restricted Internet access is simulated with a Web Filter profile that blocks [google.com](#). You will create FortiClient SSL and IPsec VPN tunnels to bypass the web filter, connect to a remote FortiGate unit, and transparently browse the Internet to [google.com](#).

The recipe assumes that a "vpn\_users" user group and a Local LAN firewall address have already been created.

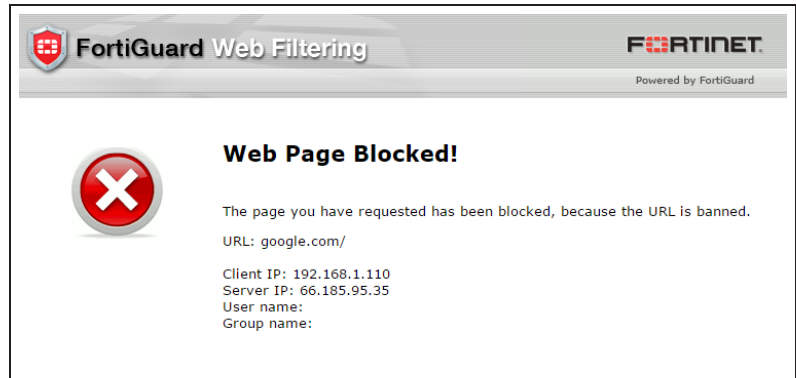
A video of this recipe is available [here](#).

## 1. Starting point

In this example, we simulate restricted Internet access using a Web Filtering profile to block Google.

With the user situated behind this FortiGate, google.com cannot be accessed, and instead the FortiGuard "Web Page Blocked" message appears.

For the user to bypass this Web Filter, the following VPN configurations must be made on a remote FortiGate (which is not blocked by any filter), and the user must connect to it using **FortiClient**.

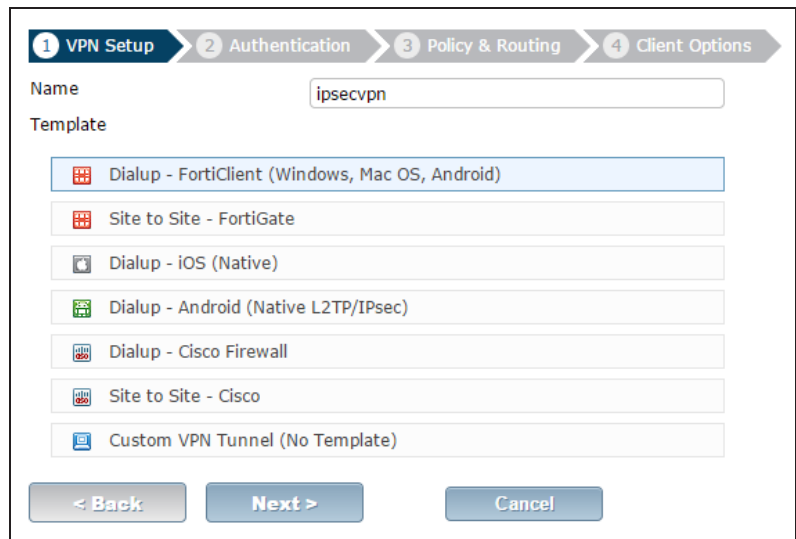


## 2. Configuring the IPsec VPN

On the remote Fortigate, go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click **Next**.

*The tunnel name must not have any spaces in it.*



Set the **Incoming Interface** to the internet-facing interface. In this case, **wan1**.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the **vpn\_users** user group, then click **Next**.

*The pre-shared key is a credential for the VPN and should differ from the user's password.*

Set **Local Interface** to the internal interface and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the \_range suffix (in this case, ipsecvpn\_range).*

*In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.*

Click **Next** and select **Client Options** as desired.

The screenshot shows the 'Authentication' step of the VPN Setup Wizard. The progress bar at the top indicates the steps: 1. VPN Setup (checked), 2. Authentication (active), 3. Policy & Routing, and 4. Client Options. The configuration is for 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. The 'Incoming Interface' is set to 'wan1'. The 'Authentication Method' is 'Pre-shared Key' (selected with a radio button). The 'Pre-shared Key' field contains seven dots, and the 'Hide Characters' checkbox is checked. The 'User Group' is set to 'vpn\_users'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'Policy & Routing' step of the VPN Setup Wizard. The progress bar at the top indicates the steps: 1. VPN Setup (checked), 2. Authentication (checked), 3. Policy & Routing (active), and 4. Client Options. The configuration is for 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. The 'Local Interface' is set to 'internal'. The 'Local Address' is set to 'Local LAN' (indicated by a green plus icon). The 'Client Address Range' is '10.10.110.1-10.10.110.10' and the 'Subnet Mask' is '255.255.255.0'. The 'DNS Server' section has 'Use System DNS' selected. The 'Enable IPv4 Split Tunnel' checkbox is unchecked, and the 'Allow Endpoint Registration' checkbox is checked. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'Client Options' step of the VPN Setup Wizard. The progress bar at the top indicates the steps: 1. VPN Setup (checked), 2. Authentication (checked), 3. Policy & Routing (checked), and 4. Client Options (active). The configuration is for 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. The 'Save Password' checkbox is checked, while 'Auto Connect' and 'Always Up (Keep Alive)' are unchecked. At the bottom are buttons for '< Back', 'Create', and 'Cancel'.

When using the IPsec VPN Wizard, an IPsec firewall address range is automatically created using the name of the tunnel you entered into the Wizard. The Wizard also creates an **IPsec -> internal** IPv4 policy, so all that is left is to create the Internet access policy. See [Step 4](#).

### 3. Configuring the SSL VPN

Go to **VPN > SSL > Portals**, highlight the **full-access** portal, and select **Edit**.

Create New Edit Delete

| Name          | Tunnel Mode | Web Mode | Ref. |  |
|---------------|-------------|----------|------|--|
| full-access   | ✓           | ✓        | 1    |  |
| tunnel-access | ✓           | ✗        | 0    |  |
| web-access    | ✗           | ✓        | 1    |  |

Disable **Split Tunneling** so that all VPN traffic will go through the FortiGate firewall.



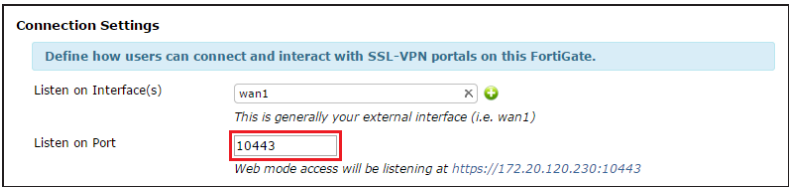
Name: full-access

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools: SSLVPN\_TUNNEL\_ADDR1

Go to **VPN > SSL > Settings**. Under **Connection Settings** set **Listen on Port** to **10443**.



**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

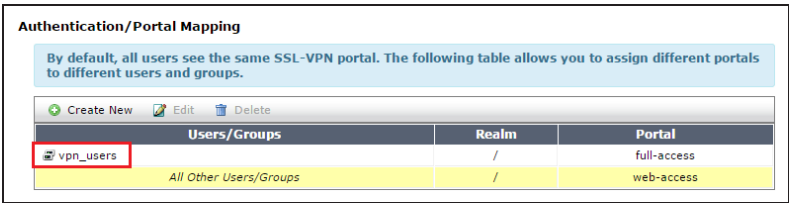
Listen on Interface(s): wan1

Listen on Port: 10443

*This is generally your external interface (i.e. wan1)*

*Web mode access will be listening at https://172.20.120.230:10443*

Under **Authentication/Portal Mapping**, assign the **vpn\_users** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal.



**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

| Create New             | Edit  | Delete      |
|------------------------|-------|-------------|
| Users/Groups           | Realm | Portal      |
| vpn_users              | /     | full-access |
| All Other Users/Groups | /     | web-access  |

By default, the FortiGate has an **ssl.root** firewall address. All that is left is to create the Internet access policy, as described in the following step.

## 4. Creating security policies for VPN access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create two security policies allowing remote users to access the Internet securely through the FortiGate unit; one for each VPN tunnel.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

For SSL VPN, set **Source User(s)** to the **vpn\_users** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

|   |                 |
|---|-----------------|
| Incoming Interface  | ipsecvpn        |
| Source Address  | all             |
| Source User(s)  | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | wan1            |
| Destination Address   | all             |
| Schedule  | always          |
| Service   | ALL             |
| Action  | ACCEPT          |
| <b>Firewall / Network Options</b>   |                 |
| <input checked="" type="checkbox"/> NAT   |                 |
| <input checked="" type="radio"/> Use Outgoing Interface Address <input type="checkbox"/> Fixed Port |                 |

|   |                              |
|---|------------------------------|
| Incoming Interface                      | ssl.root (SSL VPN interface) |
| Source Address                          | all                          |
| Source User(s)                          | vpn_users                    |
| Outgoing Interface                      | wan1                         |
| Destination Address                     | all                          |
| Schedule                                | always                       |
| Service                                 | ALL                          |
| Action                                  | ACCEPT                       |
| <b>Firewall / Network Options</b>       |                              |
| <input checked="" type="checkbox"/> NAT |                              |

## 5. Configuring FortiClient for IPsec and SSL VPN

Open FortiClient, go to **Remote Access** and add new connections for both VPNs.

|   |   |
|---|---|
| <div>AntiVirus<br/>Real-time Protection Disabled</div> <div>Parental Control<br/>4 Violations</div> <div>Remote Access<br/>No VPN Connected</div> | <div>Add a new connection</div> <div>Edit the selected connection</div> <div>Delete the selected connection</div> <div>Password</div> |
|---|---|

Provide a **Connection Name** and set the

Type to either **IPsec VPN** or **SSL VPN** depending on the VPN configuration.

Set **Remote Gateway** to the FortiGate IP address.

- For IPsec VPN, set **Authentication Method** to **Pre-Shared Key** and enter the key below.
- For SSL VPN, set **Customize Port** to **10443**.

(Optional) For **Username**, enter a username from the **vpn\_users** user group.

Edit VPN Connection

Connection Name

FortiGate\_with\_SSL

Type

☒ SSL-VPN

☐ IPsec VPN

Description

FortiGate\_with\_SSL

Remote Gateway

172.20.120.1

☒ Customize port

10443

Authentication

☐ Prompt on login

☒ Save login

Username

twhite

Client Certificate

☐

Do not Warn Invalid Server Certificate

☐

OK

Cancel

Delete

Select the new connection, enter the username and password, and click **Connect**.

AntiVirus

Real-time Protection Disabled

Parental Control

4 Violations

Remote Access

No VPN Connected

FortiGate\_with\_IPsec

twhite

Password

If prompted with a server authentication warning, select **Yes**.

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Yes

No

View Certificate

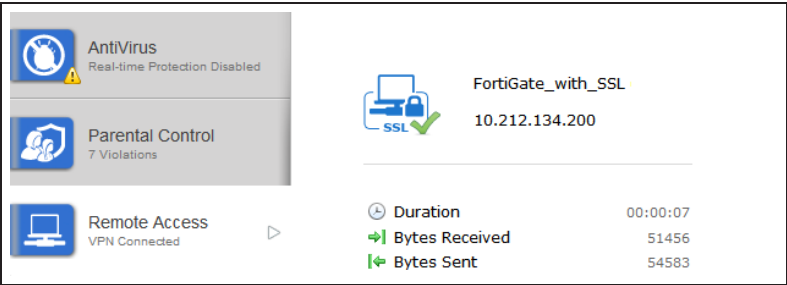
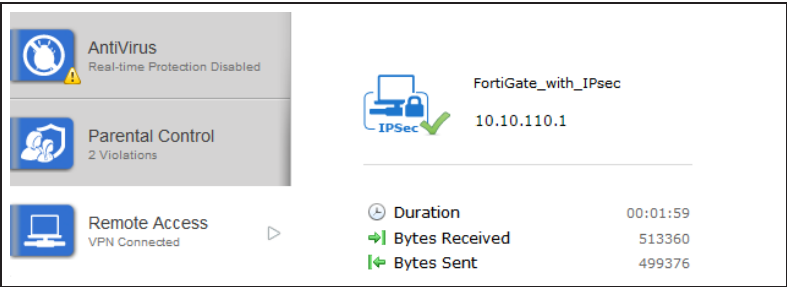
More Info

VPNs

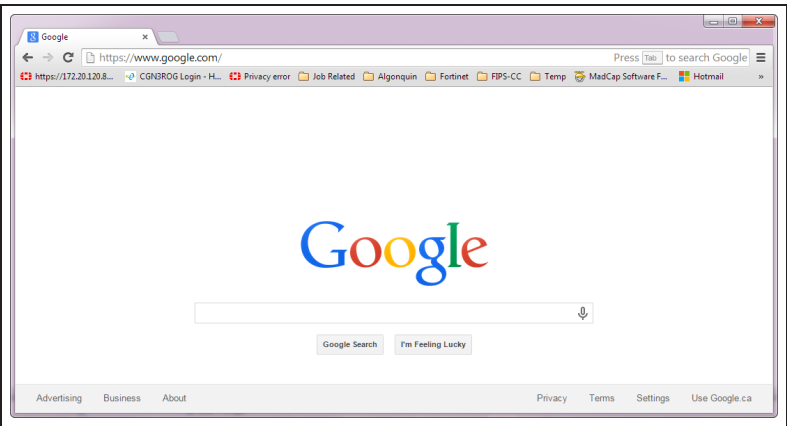
377

## 6. Results

From FortiClient start an IPsec or SSL VPN session. Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.

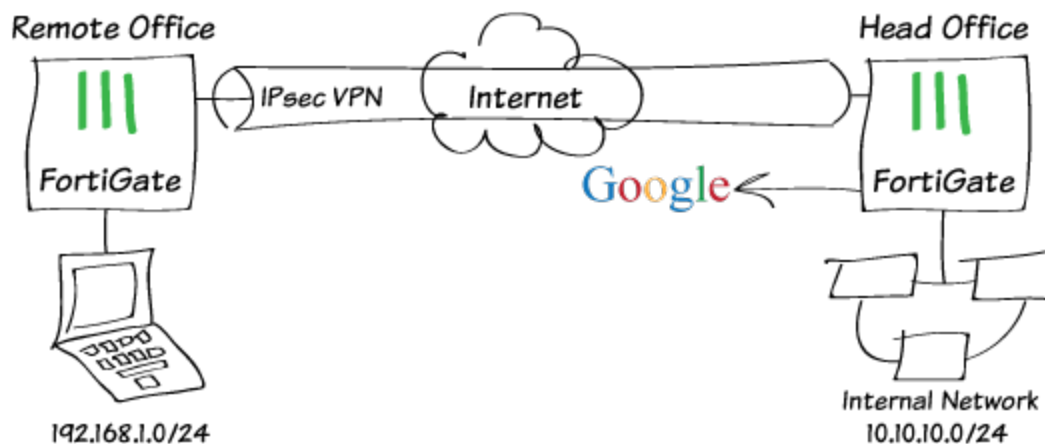


With the tunnel up, you can now visit [google.com](https://www.google.com/) without being blocked, since the Internet traffic is handled by the remote FortiGate and the web filter on the local FortiGate has been bypassed.



For further reading, check out [IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook](#).

# Remote browsing using site-to-site IPsec VPN



In this recipe, you will configure a site-to-site, also called gateway-to-gateway, IPsec VPN between an office with Internet access restrictions (Remote Office) and an office without these restrictions (Head Office) so that the Remote Office can access the Internet through the Head Office, avoiding the restrictions.

To bypass this restriction, this example shows how create a site-to-site VPN to connect the Remote Office FortiGate unit to the Head Office FortiGate unit, and allow Remote Office staff to transparently browse the Internet to google.com using the Head Office's Internet connection.

Note that both FortiGates run FortiOS firmware version 5.2.2 and have static IP addresses on Internet-facing interfaces. You will also need to know the Remote Office's gateway IP address.



## 1. Configuring IPsec VPN on the Head Office FortiGate

In a real world scenario, a Remote Office's ISP or something in their local Internet may be blocking access to Google, or any other site for that matter.

On the Head Office FortiGate, go to **VPN > IPsec > Wizard**.

Name the VPN, select **Site to Site - FortiGate**, and click **Next**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name: Head Office

Template:

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate**
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Remote Gateway** to the Remote Office FortiGate IP address

The Wizard should select the correct **Outgoing Interface** when you click anywhere else in the window. Depending on your configuration, you may have to manually set the outgoing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key then click **Next**.

*The pre-shared key is a credential for the VPN and should differ from the user's password. Both FortiGate's must have the same pre-shared key.*

1 VPN Setup 2 Authentication 3 Policy & Routing

Head Office : Site to Site - FortiGate

Remote Gateway: 10.10.20.1

Outgoing Interface: port1 ( Detected via routing lookup ) [Change]

Authentication Method: ☒ Pre-shared Key ☐ Signature

Pre-shared Key: ..... ☒ Hide Characters

< Back Next > Cancel

Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Head Office internal network.

For **Local Subnets**, enter the subnet range of the Head Office internal network. Depending on your configuration, this may be set automatically by the wizard.

For **Remote Subnets**, enter the subnet range of the Remote Office internal network then click **Create**.

The VPN Wizard informs you that a static route has been created, as well as two security policies and two address objects, which are added to two address groups (also created).

VPN Setup

Authentication

3 Policy & Routing

Head Office : Site to Site - FortiGate

Local Interface

port2

Local Subnets

10.10.10.0/24

Remote Subnets

192.168.1.0/24

< Back

Create

Cancel

VPN Setup

Authentication

Policy & Routing

Head Office : Site to Site - FortiGate

The VPN has been set up

Summary of Created Objects

Phase 1 Interface

Head Office

Phase 2 Interfaces

Head Office

Static Routes

192.168.1.0/24

Local Address Group

Head Office\_local

Remote Address Group

Head Office\_remote

Local to Remote Policy

1

Remote to Local Policy

2

Add Another

Show Tunnel List

Create a security policy to allow the Remote Office to have Internet access. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.

Set **Incoming Interface** to the VPN interface created by the VPN wizard and set **Source Address** to the remote office address group created by the VPN wizard.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **all**.

Enable **NAT** and (optionally) enforce any company security profiles.

The screenshot shows the 'Policy & Objects > Policy > IPv4' configuration window. It contains the following fields and options:

- Incoming Interface:** Head Office
- Source Address:** Head Office\_remote\_subnet\_1
- Source User(s):** Click to add...
- Source Device Type:** Click to add...
- Outgoing Interface:** port1
- Destination Address:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT
- Firewall / Network Options:**
  - ☒ **ON** NAT
  - ☒ Use Outgoing Interface Address
  - ☐ Use Dynamic IP Pool
  - ☐ Fixed Port
  - Click to add...

## 2. Adding a route on the Remote Office FortiGate

On the Remote Office FortiGate, create a static route that forwards traffic destined for the Head Office FortiGate to the ISP's Internet gateway.

(In this example, the Head Office FortiGate IP address is 172.20.120.154 so the destination IP/Mask is 172.20.120.154/255.255.255.0 and the ISP's gateway IP address is 10.10.20.100.)

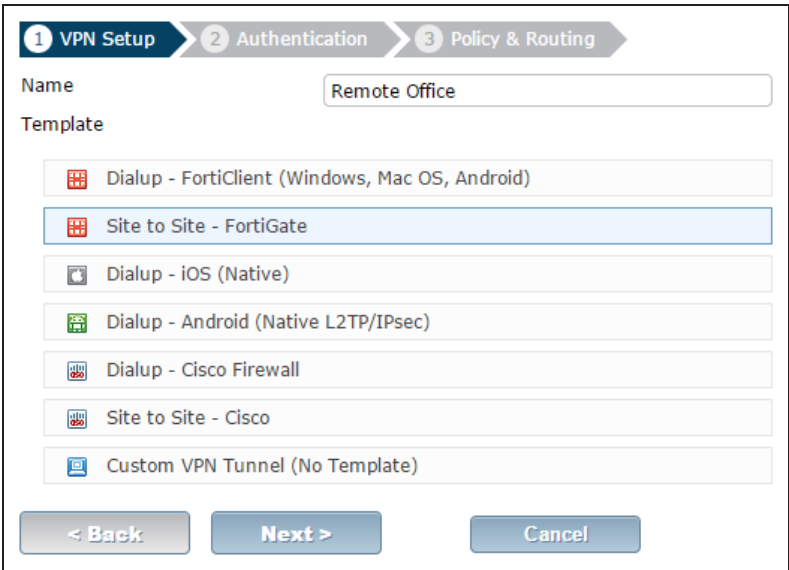
The screenshot shows the 'Static Route' configuration window. It contains the following fields and options:

- Destination IP/Mask:** 172.20.120.154/255.255
- Device:** wan1
- Gateway:** 10.10.20.100
- Administrative Distance:** 10
- Comments:** 0/255
- Advanced Options:** (collapsed)
- Buttons:** OK, Cancel

### 3. Configuring IPsec VPN on the Remote Office FortiGate

On the Remote Office FortiGate, go to **VPN > IPsec > Wizard**.

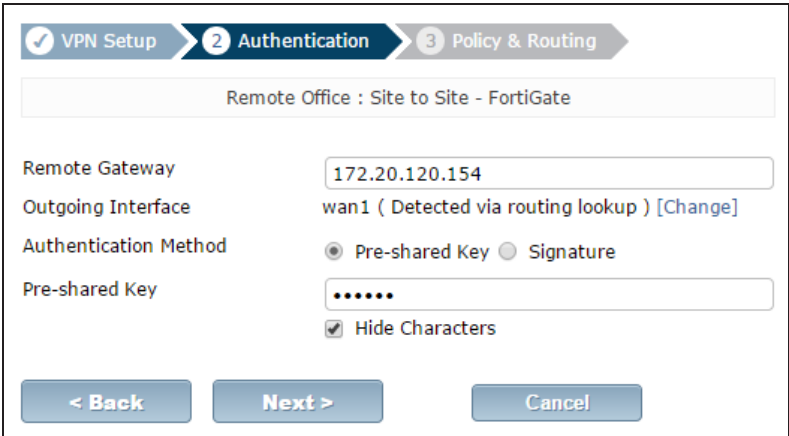
Name the VPN, select **Site to Site - FortiGate**, and click **Next**.



Set the **Remote Gateway** to the Head Office FortiGate IP address.

The Wizard should select the correct **Outgoing Interface**.

Select **Pre-shared Key** for the **Authentication Method** and enter the same **Pre-shared Key** as you entered in **Step 1**.



Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Remote Office internal network.

For **Local Subnets**, enter the subnet range of the Remote Office internal network.

For **Remote Subnets**, enter the subnet range of the Head Office internal network then click **Create**.

The VPN Wizard informs you that a static route has been created, as well as two address groups and two security policies.

VPN Setup

Authentication

3 Policy & Routing

Remote Office : Site to Site - FortiGate

Local Interface

internal1 (Local LAN)

Local Subnets

192.168.1.0/24

Remote Subnets

10.10.10.0/24

< Back

Create

Cancel

VPN Setup

Authentication

Policy & Routing

Remote Office : Site to Site - FortiGate

The VPN has been set up

Summary of Created Objects

Phase 1 Interface

Remote Office

Phase 2 Interfaces

Remote Office

Static Routes

10.10.10.0/24

Local Address Group

Remote Office\_local

Remote Address Group

Remote Office\_remote

Local to Remote Policy

2

Remote to Local Policy

3

Add Another

Show Tunnel List

Allow Internet traffic from the remote office to enter the VPN tunnel.

On the Remote Office FortiGate, go to **Policy & Objects > Policy > IPv4**.

Edit the outbound security policy created by the VPN Wizard.

Change the **Destination Address** to **all** so that the policy accepts Internet traffic.

Incoming Interface

internal1 (Local LAN)

Source Address

Remote Office\_local

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

Remote Office

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

## 4. Establishing the tunnel

On either FortiGate, go to **VPN > Monitor > IPsec Monitor**.

Right-click the newly created tunnel and select **Bring Up**.

If the tunnel is established, the **Status column** will read **Up** on both of the FortiGates.

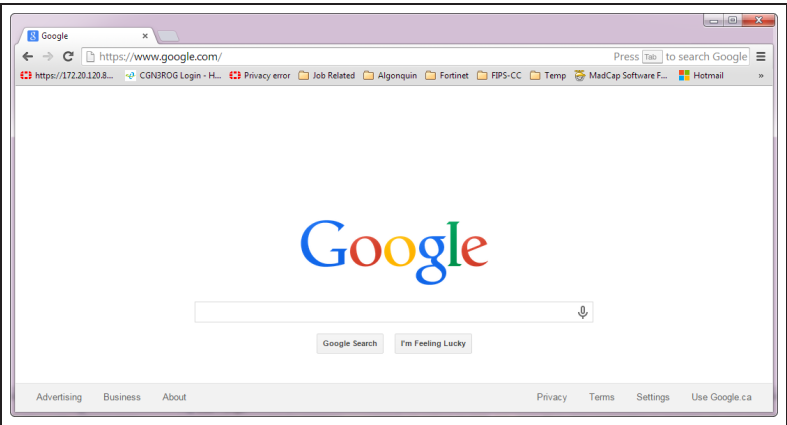
| Name          | Type                     | Remote Gateway | Username | Status | Incoming Data |
|---------------|--------------------------|----------------|----------|--------|---------------|
| Remote Office | Site to Site - FortiGate | 172.20.120.154 |          | Down   |               |

[Reset Statistics](#)  
[Bring Up](#)  
[Bring Down](#)

| Name          | Type                     | Remote Gateway | Username | Status |
|---------------|--------------------------|----------------|----------|--------|
| Remote Office | Site to Site - FortiGate | 172.20.120.154 |          | Up     |

## 6. Results

With the tunnel up, you can now visit [google.com](https://www.google.com/) without being blocked, since the Internet traffic is handled by the Head Office FortiGate and the access restrictions on the remote FortiGate have been bypassed.



For further reading, check out [IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook](#).

# IPsec troubleshooting

This section contains tips to help you with some common challenges of IPsec VPNs.

## The options to configure policy-based IPsec VPN are unavailable.

Go to **System > Config > Features**. Select Show More and turn on Policy-based IPsec VPN.

## The VPN connection attempt fails.

If your VPN fails to connect, check the following:

- Ensure that the pre-shared keys match exactly.
- Ensure that both ends use the same P1 and P2 proposal settings.
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.
- Ensure that your FortiGate unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly on the FortiGate and that clients have specified the correct Local ID.
- If you are using FortiClient, ensure that your version is compatible with the FortiGate firmware by reading the FortiOS Release Notes.
- Ensure that the Quick Mode selectors are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range.
- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the FortiGate unit is set to Enable as Server.
- If your FortiGate unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your FortiGate unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the diagnostic command in the CLI:

```
diag debug application ike -ldiag debug enable
```

The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

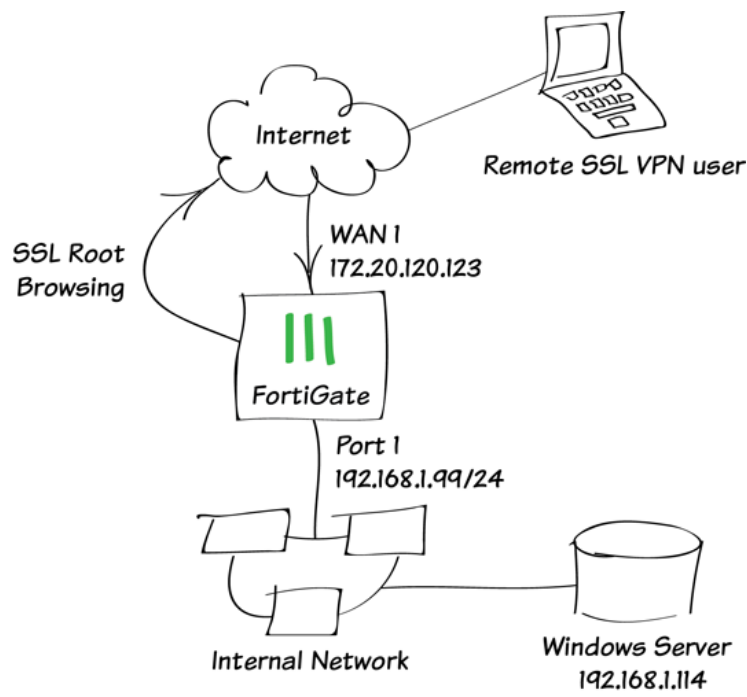
```
diag debug resetdiag debug disable
```

## The VPN tunnel goes down frequently.

If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.



# SSL VPN for remote users



This example provides remote users with access to the corporate network using SSL VPN and connect to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user’s antivirus software is installed and current.

A video of this recipe can be found [here](#).

## 1. Creating an SSL VPN portal for remote users

Go to **VPN > SSL > Portals**.

Edit the **full-access** portal. The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

The screenshot shows the configuration window for the 'full-access' SSL VPN portal. The 'Name' field is set to 'full-access'. Under 'Enable Tunnel Mode', 'Enable Tunnel Mode' is checked, while 'Enable Split Tunneling' is unchecked. The 'Source IP Pools' field contains 'SSLVPN\_TUNNEL\_ADDR1'. Under 'Enable IPv6 Tunnel Mode', 'Enable IPv6 Tunnel Mode' is checked, while 'Enable IPv6 Split Tunneling' is unchecked. The 'Source IPv6 Pools' field contains 'SSLVPN\_TUNNEL\_IPv6\_ADDR1'. Under 'Client Options', 'Save Password', 'Auto Connect', and 'Always Up (Keep Alive)' are all unchecked. Under 'Enable Web Mode', 'Enable Web Mode' is checked. The 'Portal Message' is 'Welcome to SSL VPN Service', the 'Theme' is 'Blue', and the 'Page Layout' is set to a two-column view. A list of checkboxes includes 'Include Status Information', 'Include Connection Tool', 'Include FortiClient Download', 'Prompt Mobile Users to Download FortiClient Application', 'Include Login History', and 'Enable User Bookmarks'. The 'Predefined Bookmarks' section shows a table with columns 'Name', 'Type', 'Location', and 'Description', and a message 'No matching entries found'. At the bottom, there is a checkbox for 'Limit Users to One SSL-VPN Connection at a Time' and 'OK' and 'Cancel' buttons.

Name: full-access

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools: SSLVPN\_TUNNEL\_ADDR1

☒ Enable IPv6 Tunnel Mode

☐ Enable IPv6 Split Tunneling

Source IPv6 Pools: SSLVPN\_TUNNEL\_IPv6\_ADDR1

Client Options

☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

☒ Enable Web Mode

Portal Message: Welcome to SSL VPN Service

Theme: Blue

Page Layout:

☒ Include Status Information

☒ Include Connection Tool

☒ Include FortiClient Download

☒ Prompt Mobile Users to Download FortiClient Application

☐ Include Login History

☒ Enable User Bookmarks

**Predefined Bookmarks**

| Name                      | Type | Location | Description |
|---------------------------|------|----------|-------------|
| No matching entries found |      |          |             |

☐ Limit Users to One SSL-VPN Connection at a Time

OK Cancel

Select **Create New** in the Predefined Bookmarks area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.

New Bookmark

Category

Remote Desktop

Name

Windows Server

Type

RDP

Host

192.168.1.114

Screen Width

1024

Screen Height

768

Full Screen Mode

☒

Username

twhite

Password

•••••

Keyboard Layout

English, US.

Description

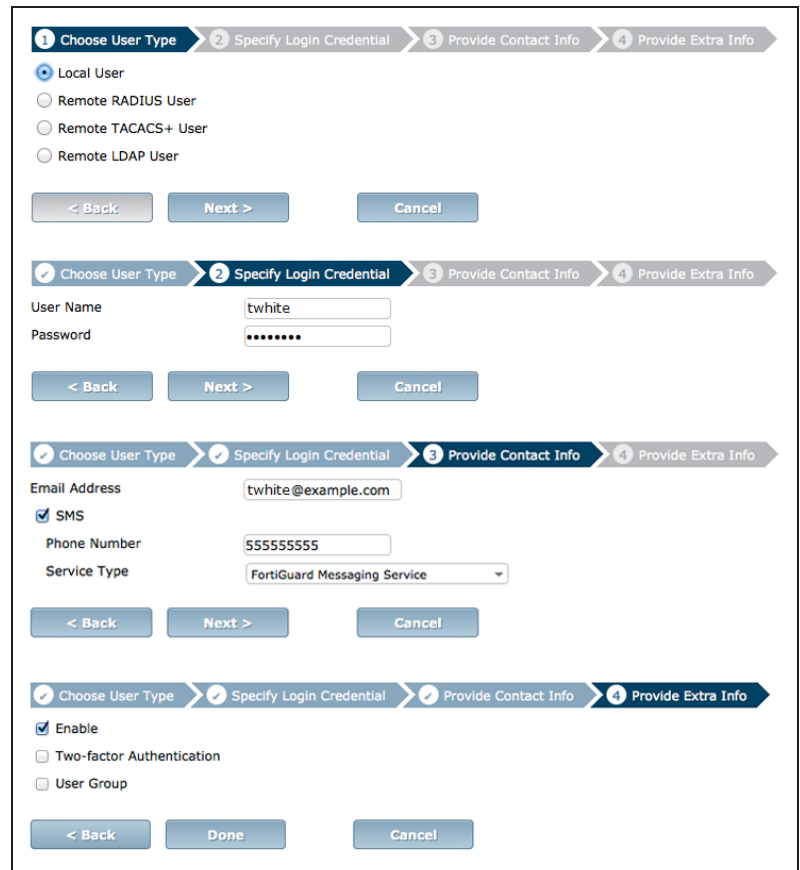
OK

Cancel

## 2. Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the **User Creation Wizard** (in the example, *twhite*, with the same credentials used for the predefined bookmark).



The image shows the User Creation Wizard with four steps:

- 1 Choose User Type**: Local User (selected), Remote RADIUS User, Remote TACACS+ User, Remote LDAP User. Buttons: < Back, Next >, Cancel.
- 2 Specify Login Credential**: User Name: twhite, Password: [masked]. Buttons: < Back, Next >, Cancel.
- 3 Provide Contact Info**: Email Address: twhite@example.com, SMS (checked), Phone Number: 55555555, Service Type: FortiGuard Messaging Service. Buttons: < Back, Next >, Cancel.
- 4 Provide Extra Info**: Enable (checked), Two-factor Authentication (unchecked), User Group (unchecked). Buttons: < Back, Done, Cancel.

Go to **User & Device > User > User Groups**.

Add the user *twhite* to a user group for SSL VPN connections.



The image shows the User Groups configuration page:

- Name: sslvpn\_group
- Type (RSSO): Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On
- Members: twhite (with add icon)
- Remote groups: Add, Edit, Delete buttons. Table with columns: Remote Server, Group Name. Message: No matching entries found.
- Buttons: OK, Cancel.

### 3. Adding an address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add the address for the local network.  
Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Visibility

☒

Comments

Write a comment... 0/255

OK

Cancel

### 4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to wan1.

Set **Listen on Port** to **443** and **Specify custom IP ranges**.

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

wan1

This is generally your external interface (i.e. wan1)

Listen on Port

443

Restrict Access

☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout

☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For

5000 (Seconds)

Server Certificate

Fortinet\_Factory

Require Client Certificate

☐

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range

☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges

SSLVPN\_TUNNEL\_ADDR1

SSLVPN\_TUNNEL\_IPv6\_ADDR1

Under **Authentication/Portal Mapping**, add the SSL VPN user group.

| Create New             | Edit  | Delete      |
|------------------------|-------|-------------|
| Users/Groups           | Realm | Portal      |
| sslvpn_group           | /     | full-access |
| All Other Users/Groups | /     | web-access  |

## 5. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** group you created in step 2.

Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.

Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

|  |                                     |
|--|-------------------------------------|
| Incoming Interface   | ssl.root (sslvpn tunnel interface)  |
| Source Address   | all                                 |
| Source User(s)   | sslvpn_group                        |
| Source Device Type   | Click to add...                     |
| Outgoing Interface   | lan                                 |
| Destination Address  | all                                 |
| Schedule   | always                              |
| Service  | ALL                                 |
| Action   | ACCEPT                              |
| <b>Firewall / Network Options</b>                                  |                                     |
| <input checked="" type="checkbox"/> NAT                            |                                     |
| <input checked="" type="radio"/> Use Destination Interface Address | <input type="checkbox"/> Fixed Port |
| <input type="radio"/> Use Dynamic IP Pool                          | Click to add...                     |
| <input type="radio"/> Use Central NAT Table                        |                                     |

|                     |                                    |
|---------------------|------------------------------------|
| Incoming Interface  | ssl.root (sslvpn tunnel interface) |
| Source Address      | all                                |
| Source User(s)      | Click to add...                    |
| Source Device Type  | Click to add...                    |
| Outgoing Interface  | wan1                               |
| Destination Address | all                                |
| Schedule            | always                             |
| Service             | ALL                                |
| Action              | ACCEPT                             |

## 6. Setting the FortiGate unit to verify users have current AntiVirus software

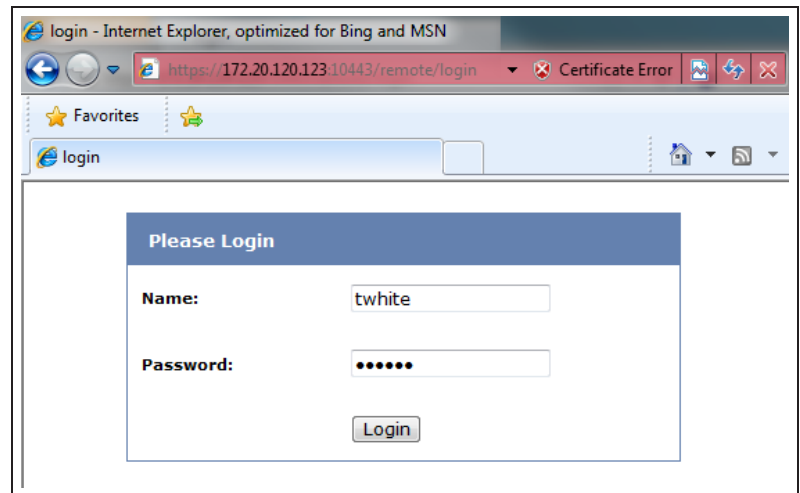
Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant AntiVirus software on the remote user's computer.

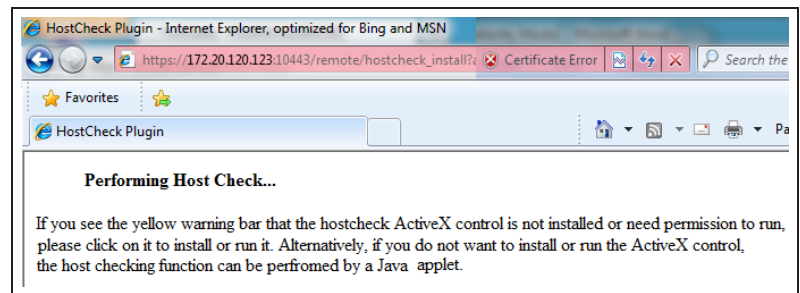
```
config vpn ssl web portal
edit full-access
set host-check av
end
end
```

## 7. Results

Log into the portal using the credentials you created in step 2.

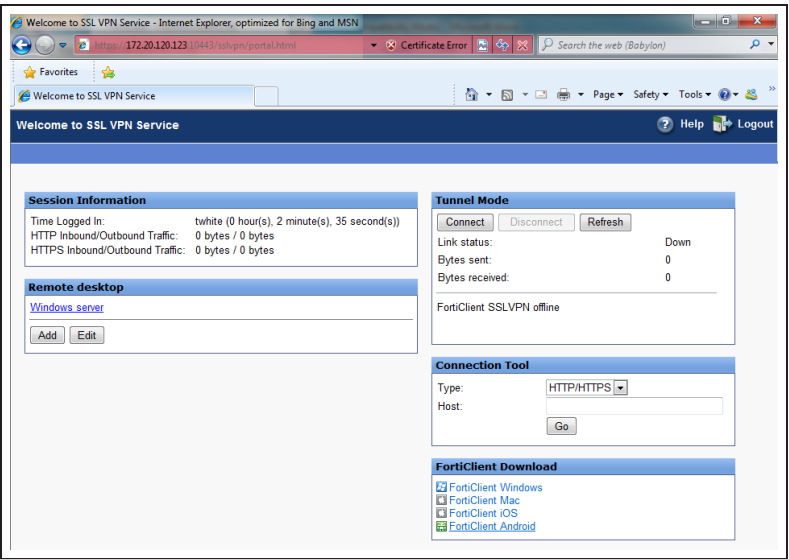


The FortiGate unit performs the host check.

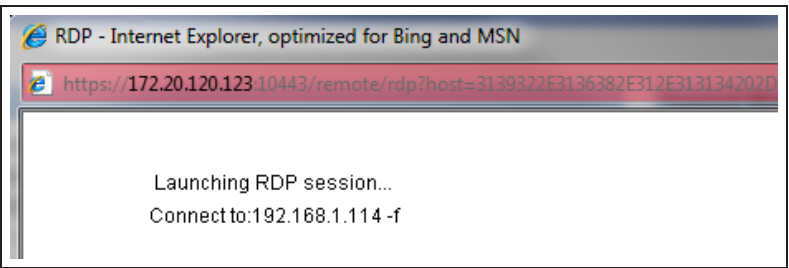


After the check is complete, the portal appears.

*You may need to install the FortiClient application using the available download link.*



Select the bookmark **Remote Desktop** link to begin an RDP session.






Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

| Delete                   |            |       |                                   |                          |             |
|--------------------------|------------|-------|-----------------------------------|--------------------------|-------------|
|                          | No.        | User  | Source IP                         | Begin Time               | Description |
| <input type="checkbox"/> | 1          | twite | 172.20.120.23                     | Wed Apr 17 11:41:06 2013 |             |
| <input type="checkbox"/> | Subsession |       | Web Application:RDP 192.168.1.114 |                          |             |



Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

|                     |  |                     |   |
|---------------------|--|---------------------|---|
| Dst                 | 192.168.1.114  | Virtual Domain      | root  |
| Received            | 85591  | Source Country      | Reserved  |
| Sent / Received     | 8.71 KB / 83.58 KB   | Duration            | 36  |
| Sent                | 8923   | Application Details |   |
| Group               | N/A  | Service             | RDP   |
| Protocol            | 6  | User                |  twwhite                 |
| Destination Country | Reserved   | Dst Port            | 3389  |
| roll                | 65389  | Status              | ✓   |
| Timestamp           | Wed Apr 17 14:13:11 2013   | Tran Display        | noop  |
| Sequence Number     | 2700   | Policy ID           | 11  |
| Src Interface       | wan1   | Src                 |  twwhite (172.20.120.23) |
| VPN                 | sslvpn_web_mode  | Sent Packets        | 71  |
| Level               | notice  | VPN Type            | sslvpn  |
| Src Port            | 53712  | Log ID              | 13  |
| Sub Type            | forward  | Threat              |   |
| Received Packets    | 98   | Date/Time           | 14:13:11 (Wed Apr 17 14:13:11 2013)   |
| Dst Interface       | port1  |                     |   |

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.

Tunnel Mode

Connect

Disconnect

Refresh

Link status:

Up

Bytes sent:

46865


Bytes received:


118096


FortiClient SSLVPN connected to server

Select the bookmark **Remote Desktop** link to begin an RDP session.

RDP - Internet Explorer, optimized for Bing and MSN

 https://172.20.120.123:10443/remote/rdp?host=31393

 Certificate Error






Launching RDP session...  
Connect to:192.168.1.114 -f

Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.










Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

| Delete                   |     |            |               |                          |                          |
|--------------------------|-----|------------|---------------|--------------------------|--------------------------|
|                          | No. | User       | Source IP     | Begin Time               | Description              |
| <input type="checkbox"/> | 1   | twhite     | 172.20.120.23 | Wed Apr 17 11:41:06 2013 |                          |
| <input type="checkbox"/> |     | Subsession |               |                          | Tunnel IP:10.212.134.200 |



|                            |  |                            |  |
|----------------------------|--|----------------------------|--|
| <b>Dst</b>                 | 192.168.1.114  | <b>Virtual Domain</b>      | root   |
| <b>Received</b>            | 326664   | <b>Source Country</b>      | Reserved   |
| <b>Sent / Received</b>     | 54.36 KB / 319.01 KB   | <b>Duration</b>            | 83   |
| <b>Sent</b>                | 55665  | <b>Application Details</b> |  |
| <b>Group</b>               | N/A  | <b>Service</b>             | RDP  |
| <b>Protocol</b>            | 6  | <b>User</b>                |  twhite                 |
| <b>Destination Country</b> | Reserved   | <b>Dst Port</b>            | 3389   |
| <b>roll</b>                | 65389  | <b>Status</b>              | ✓  |
| <b>Timestamp</b>           | Wed Apr 17 14:17:15 2013   | <b>Tran Display</b>        | noop   |
| <b>Sequence Number</b>     | 3618   | <b>Policy ID</b>           | 11   |
| <b>Src Interface</b>       | wan1   | <b>Src</b>                 |  twhite (172.20.120.23) |
| <b>VPN</b>                 | sslvpn_web_mode  | <b>Sent Packets</b>        | 329  |
| <b>Level</b>               | notice  | <b>VPN Type</b>            | sslvpn   |
| <b>Src Port</b>            | 53820  | <b>Log ID</b>              | 13   |
| <b>Sub Type</b>            | forward  | <b>Threat</b>              |  |
| <b>Received Packets</b>    | 407  | <b>Date/Time</b>           | 14:17:15 (Wed Apr 17 14:17:15 2013)  |
| <b>Dst Interface</b>       | unknown-0  |                            |  |

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

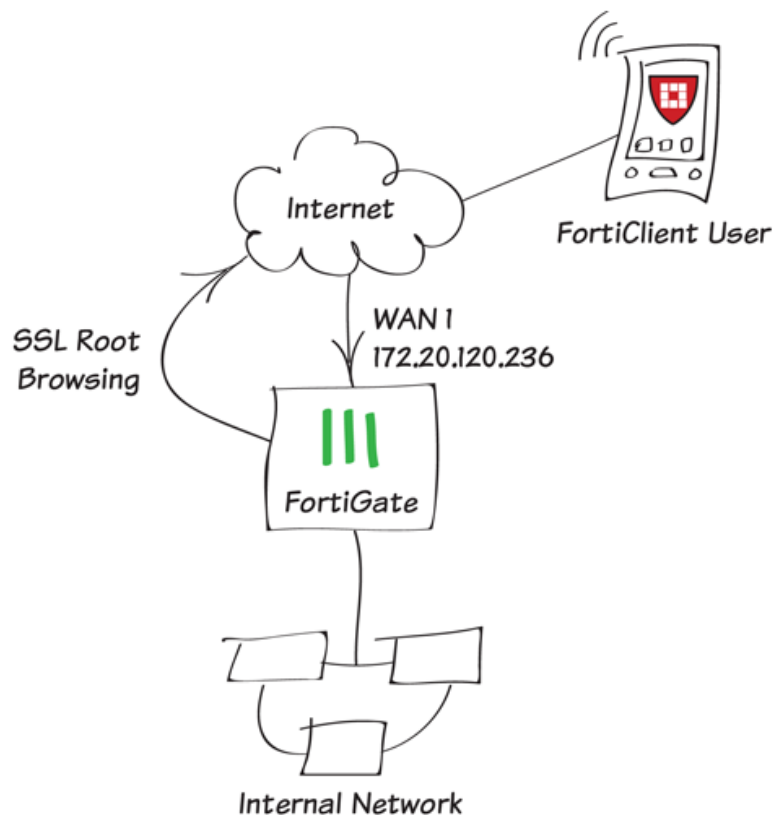
| Refresh Download Raw Log Log location: Disk |           |               |               |                |  |           |           |                   |  |
|---|-----------|---------------|---------------|----------------|--|-----------|-----------|-------------------|--|
| #   | Date/Time | Src Interface | Dst Interface | Src            | Dst  | Service   | Policy ID | Sent / Received   |  |
| 1   | 14:26:05  | ssl.root      | wan1          | 10.212.134.200 |  74.125.133.95                   | HTTP      | 8         | 168 B / 88 B      |  |
| 2   | 14:26:04  | ssl.root      | wan1          | 10.212.134.200 |  173.194.77.94                  | HTTP      | 8         | 168 B / 88 B      |  |
| 3   | 14:26:04  | ssl.root      | wan1          | 10.212.134.200 |  173.194.43.79                  | HTTP      | 8         | 168 B / 88 B      |  |
| 4   | 14:26:03  | ssl.root      | wan1          | 10.212.134.200 |  66.171.121.34 (fortinet.com)   | HTTP      | 8         | 535 B / 938 B     |  |
| 5   | 14:25:57  | ssl.root      | wan1          | 10.212.134.200 |  74.121.50.17 (www.pages03.net) | HTTP      | 8         | 880 B / 537 B     |  |
| 6   | 14:25:44  | ssl.root      | wan1          | 10.212.134.200 |  208.91.113.212                 | HTTPS     | 8         | 3.30 KB / 7.44 KB |  |
| 7   | 14:25:40  | ssl.root      | wan1          | 10.212.134.200 | 192.168.55.30  | KERBEROS  | 8         | 520 B / 1.64 KB   |  |
| 8   | 14:25:40  | ssl.root      | wan1          | 10.212.134.200 | 192.168.55.30  | KERBEROS  | 8         | 1.71 KB / 321 B   |  |
| 9   | 14:25:40  | ssl.root      | wan1          | 10.212.134.200 | 192.168.55.30  | KERBEROS  | 8         | 404 B / 367 B     |  |
| 10  | 14:24:39  | ssl.root      | wan1          | 10.212.134.200 |  213.199.179.159                | 40031/tcp | 8         | 512 B / 469 B     |  |
| 11  | 14:24:37  | ssl.root      | wan1          | 10.212.134.200 |  213.199.179.159                | HTTP      | 8         | 168 B / 128 B     |  |
| 12  | 14:24:37  | ssl.root      | wan1          | 10.212.134.200 |  132.246.2.6 (www.msftncsi.com) | HTTP      | 8         | 305 B / 387 B     |  |

Select an entry to view more information.

|                     |  |                     |  |
|---------------------|--|---------------------|--|
| Dst                 |  66.171.121.34 (fortinet.com) | Virtual Domain      | root   |
| Received            | 938  | Source Country      | Reserved   |
| Src NAT IP          | 172.20.120.123   | Sent / Received     | 535 B / 938 B  |
| Duration            | 17   | Sent                | 535  |
| Src NAT Port        | 54165  | Application Details |  |
| Service             | HTTP   | Protocol            | 6  |
| Destination Country | United States  | Dst Port            | 80   |
| roll                | 65389  | Status              | close  |
| Timestamp           | Wed Apr 17 14:26:03 2013   | Tran Display        | snat   |
| Sequence Number     | 8096   | Policy ID           | 8  |
| Src Interface       | ssl.root   | Src                 | 10.212.134.200   |
| Sent Packets        | 6  | Level               | notice  |
| Src Port            | 54165  | Log ID              | 13   |
| Sub Type            | forward  | Threat              |  |
| Received Packets    | 5  | Date/Time           | 14:26:03 (Wed Apr 17 14:26:03 2013)  |
| Dst Interface       | wan1   |                     |  |

For further reading, check out [Basic SSL VPN configuration](#) in the [FortiOS 5.2 Handbook](#).

# SSL VPN using FortiClient for iOS



In this recipe, you will create an SSL VPN that remote users connect to using FortiClient running on iOS.

When a user using an iOS device connects to this SSL VPN, they can access servers and data on the internal network. They can also securely browse the Internet using the FortiGate's Internet connection.

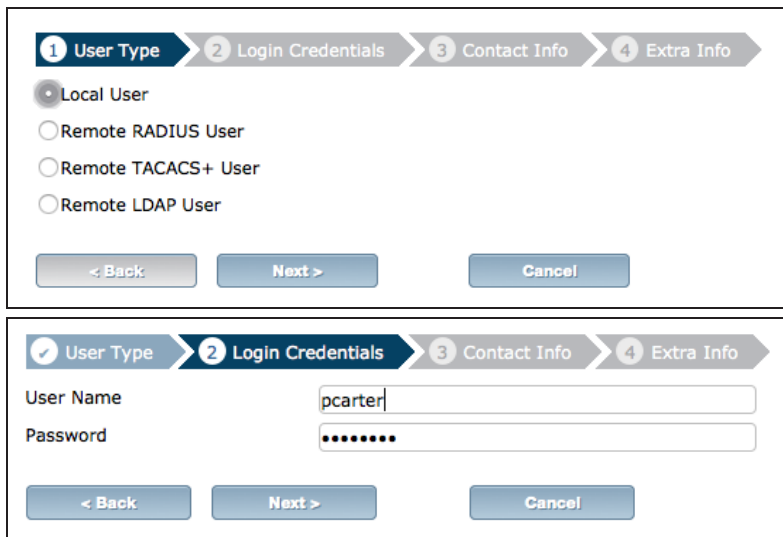
This example uses FortiClient 5.2.0.028 for iOS. FortiClient can be downloaded from [www.forticlient.com](http://www.forticlient.com).

A video of this recipe is available [here](#).

## 1. Creating users and a user group

Go to **User & Device > User > User Definition**.

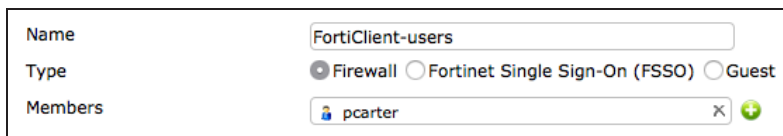
Add as many local users as required with the **User Creation Wizard**.



The image shows the 'User Type' step of the User Creation Wizard. At the top, there are four tabs: '1 User Type', '2 Login Credentials', '3 Contact Info', and '4 Extra Info'. The '1 User Type' tab is selected. Below the tabs, there are four radio button options: 'Local User' (selected), 'Remote RADIUS User', 'Remote TACACS+ User', and 'Remote LDAP User'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Go to **User & Device > User > User Groups**.

Create a user group for FortiClient users and add the new user(s) to the group.



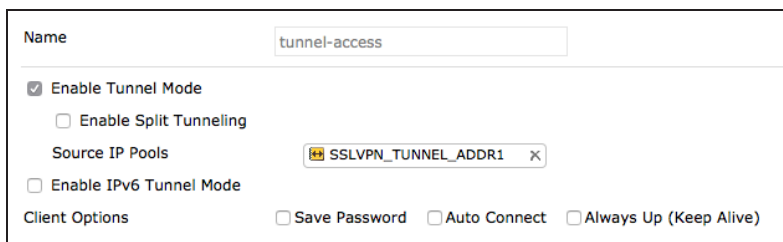
The image shows the 'User Groups' configuration page for a group named 'FortiClient-users'. It has three fields: 'Name' (FortiClient-users), 'Type' (Firewall selected, Fortinet Single Sign-On (FSSO) and Guest are unselected), and 'Members' (pccarter selected, with a plus icon to add more).

## 2. Creating an SSL VPN portal

Go to **VPN > SSL > Portals**.

Edit the **tunnel-access** portal. This portal supports tunnel mode by default.

**Enable Split Tunneling** is *not* enabled so that all SSL VPN traffic will go through the FortiGate unit.



The image shows the 'tunnel-access' portal configuration page. It has a 'Name' field with 'tunnel-access'. Below it, there are several options: 'Enable Tunnel Mode' (checked), 'Enable Split Tunneling' (unchecked), 'Source IP Pools' (SSLVPN\_TUNNEL\_ADDR1), 'Enable IPv6 Tunnel Mode' (unchecked), and 'Client Options' (Save Password, Auto Connect, Always Up (Keep Alive) all unchecked).

### 3. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to wan1.

Set **Listen on Port** to 10443 and **Specify custom IP ranges**. Use the default **IP Range**, `SSLVPN_TUNNEL_ADDR1`.

At the bottom of the page, under **Authentication/Portal Mapping**, add the FortiClient user group.

If necessary, map a portal for **All Other Users/Groups**.

Connection Settings

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

wan1

This is generally your external interface (i.e. wan1)

Listen on Port

10443

Web mode access will be listening at https://172.20.120.236:10443

Restrict Access

☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout

☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For

300 (Seconds)

Server Certificate

Self-Signed

Require Client Certificate

☐

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range

☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges

SSLVPN\_TUNNEL\_ADDR1

DNS Server

☒ Same as client system DNS ☐ Specify

Specify WINS Servers

☐

Allow Endpoint Registration

☐

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

| Create New             | Edit          | Delete |
|------------------------|---------------|--------|
| Users/Groups           | Portal        |        |
| FortiClient-users      | tunnel-access |        |
| All Other Users/Groups | web-access    |        |

## 4. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**. Create a security policy allowing SSL VPN user to access the internal network.

Set **Incoming Interface** to **ssl.root**. Set **Source Address** to **all** and **Source User** to the new user group. Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to all, enable **NAT**, and configure any remaining firewall and security options as desired.

Add a second security policy allowing SSL VPN users to access the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

|   |  |   |
|---|--|---|
| Incoming Interface  | ssl.root (SSL VPN interface)                 | + |
| Source Address  | all  | + |
| Source User(s)  | FortiClient-users                            | + |
| Outgoing Interface  | lan  | + |
| Destination Address   | all  | + |
| Schedule  | always                                       |   |
| Service   | ALL  | + |
| Action  | ACCEPT                                       |   |
| <b>Firewall / Network Options</b>                               |  |   |
| <input checked="" type="checkbox"/> NAT                         |  |   |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port          |   |
| <input type="radio"/> Use Dynamic IP Pool                       | <input type="text" value="Click to add..."/> |   |

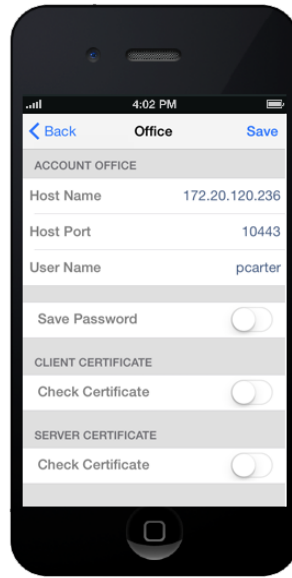
|   |  |   |
|---|--|---|
| Incoming Interface  | ssl.root (SSL VPN interface)                 | + |
| Source Address  | all  | + |
| Source User(s)  | FortiClient-users                            | + |
| Outgoing Interface  | wan1   | + |
| Destination Address   | all  | + |
| Schedule  | always                                       |   |
| Service   | ALL  | + |
| Action  | ACCEPT                                       |   |
| <b>Firewall / Network Options</b>                               |  |   |
| <input checked="" type="checkbox"/> NAT                         |  |   |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port          |   |
| <input type="radio"/> Use Dynamic IP Pool                       | <input type="text" value="Click to add..."/> |   |

## 5. Configuring FortiClient for SSL VPN in iOS

Install **FortiClient** on the iOS device.

Add a new VPN Gateway.

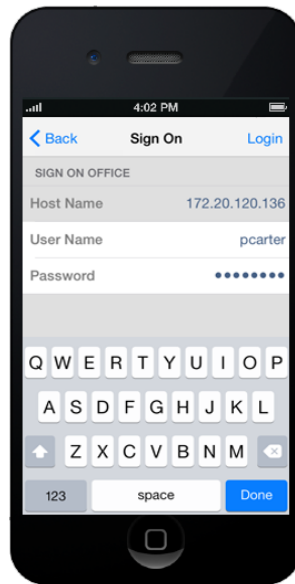
Set **Host Name** to the FortiGate's IP (in the example, *172.20.120.236*), set **Host Port** to *10443*, and set **User Name** to match the new user account.



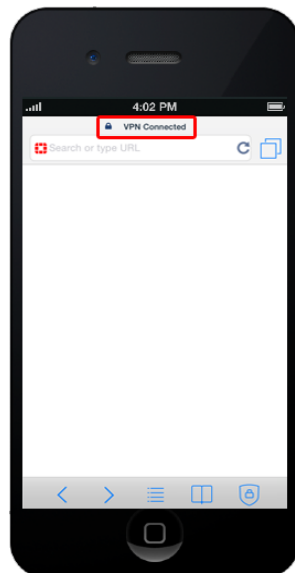


## 6. Results

Select the VPN in FortiClient. Enter the **Password** and select **Login**.



You will be able to connect to the VPN.

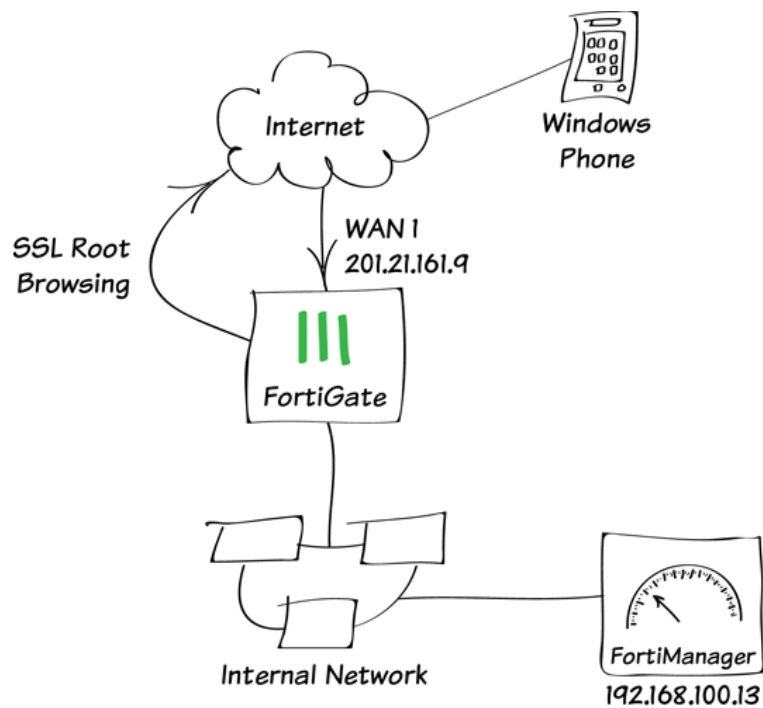


On the FortiGate, go to **VPN > Monitor > SSL-VPN Monitor** to see that the user has connected.

| <input type="checkbox"/> | No. | User    | Source IP      | Begin Time               |
|--------------------------|-----|---------|----------------|--------------------------|
| <input type="checkbox"/> | 1   | pcarter | 172.20.130.254 | Thu Jan 15 10:44:34 2015 |

For further reading, check out [FortiClient](#) in the [FortiOS 5.2 Handbook](#).

# SSL VPN for Windows Phone 8.1



In this example, you will connect to a private network with a Windows Phone, using an SSL VPN.

# 1. Creating a VPN portal with custom bookmarks

Go to **VPN > SSL > Portals** and create a new portal.

Enable both **Tunnel Mode** and **Web Mode**. Disable **Split Tunneling** and set **Source IP Pools** to use the default SSL VPN tunnel address range.

Under **Predefined Bookmarks**, create bookmarks to access resources on the internal network.

Name

PORTAL\_PBI

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools

SSLVPN\_TUNNEL\_ADDR1 X

Client Options

☐ Save Password

☒ Auto Connect

☒ Always Up (Keep Alive)

☒ Enable Web Mode

Portal Message

Bem-Vindo a VPN SSL - FGT\_110C

Theme

Blue

Page Layout

☒ Include Status Information

☒ Include Connection Tool

☐ Include FortiClient Download

☐ Prompt Mobile Users to Download FortiClient Application

☐ Include Login History

☒ Enable User Bookmarks

Predefined Bookmarks

Create NewEditDelete

| Name                 | Type       | Location        | Description     |
|----------------------|------------|-----------------|-----------------|
| WEB_APPS (6)         |            |                 |                 |
| FortiAnalyzer_WEB    | HTTP/HTTPS | 192.168.100.12  | 192.168.100.12  |
| FortiManager_WEB     | HTTP/HTTPS | 192.168.100.13  | 192.168.100.13  |
| VMWare_ESXi          | HTTP/HTTPS | 192.168.100.150 | 192.168.100.150 |
| Windows Server 20... | RDP Native | 192.168.100.10  |                 |
| Fortigate_SSH        | SSH        | 192.168.100.1   | 192.168.100.1   |
| SERVER_FTP           | FTP        | 192.168.100.10  | 192.168.100.10  |

☐ Limit Users to One SSL-VPN Connection at a Time

## 2. Creating a user and user group

Go to **User & Device > User > User Definition** and create a new local user.

The wizard consists of four steps: 1. Choose User Type, 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info.

**Step 1: Choose User Type**

- ☒ Local User
- ☐ Remote RADIUS User
- ☐ Remote TACACS+ User
- ☐ Remote LDAP User

**Step 2: Specify Login Credential**

User Name:

Password:

**Step 3: Provide Contact Info**

Email Address:

☒ SMS

Phone Number:

Service Type:

**Step 4: Provide Extra Info**

☒ Enable

☐ Two-factor Authentication

☐ User Group

Go **User & Device > User > User Groups** and create a new user group. Set **Members** to include the new user.

Name:

Type (RSSO): ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On

Members:

Remote groups:

| Remote Server             | Group Name |
|---------------------------|------------|
| No matching entries found |            |

OK Cancel

### 3. Configuring the VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **10443** and **Specify custom IP ranges** using the default SSL VPN tunnel addresses.

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

wan1

This is generally your external interface (i.e. wan1)

Listen on Port

10443

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout

Logout users when inactive for specified period

Never logout inactive users

Inactive For

5000

(Seconds)

Server Certificate

Fortinet\_Factory

Require Client Certificate

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range

Automatically assign addresses

Specify custom IP ranges

IP Ranges

SSLVPN\_TUNNEL\_ADDR1

SSLVPN\_TUNNEL\_IPv6\_ADDR1

Under **Authentication/Portal Mapping**, add the new user group.

Create New Edit Delete

| Users/Groups           | Realm | Portal      |
|------------------------|-------|-------------|
| sslvpn_group           | /     | full-access |
| All Other Users/Groups | /     | web-access  |

### 4. Creating security policies

Go to **Policy & Objects > Policy > IPv4**.

Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** new user group.

Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.

Incoming Interface

ssl.root (sslvpn tunnel interface)

Source Address

all

Source User(s)

sslvpn\_group

Source Device Type

Click to add...

Outgoing Interface

lan

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Destination Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

Use Central NAT Table

Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to your Internet-facing interface.

|                     |                                    |
|---------------------|------------------------------------|
| Incoming Interface  | ssl.root (sslvpn tunnel interface) |
| Source Address      | all                                |
| Source User(s)      | Click to add...                    |
| Source Device Type  | Click to add...                    |
| Outgoing Interface  | wan1                               |
| Destination Address | all                                |
| Schedule            | always                             |
| Service             | ALL                                |
| Action              | ACCEPT                             |

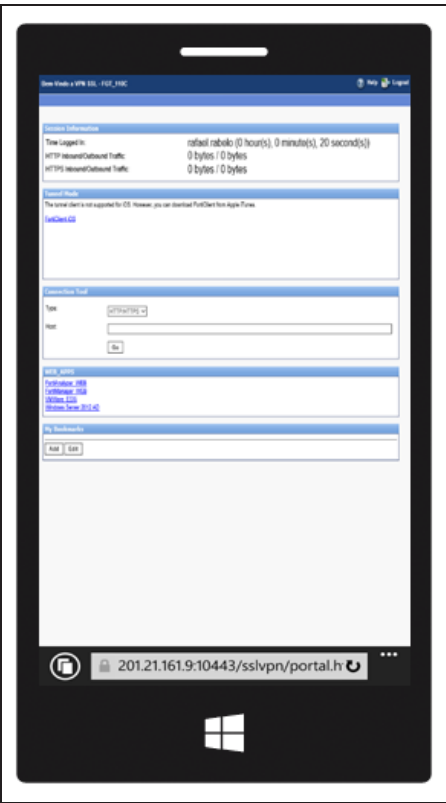
### 3. Results

Using your Window Phone's web browser, access the portal. The portal's address is the IP address of your Internet-facing interface with the port the SSL VPN tunnel is listening to, and it must be accessed using HTTPS (in the example, *https://201.21.161.9:10443*).

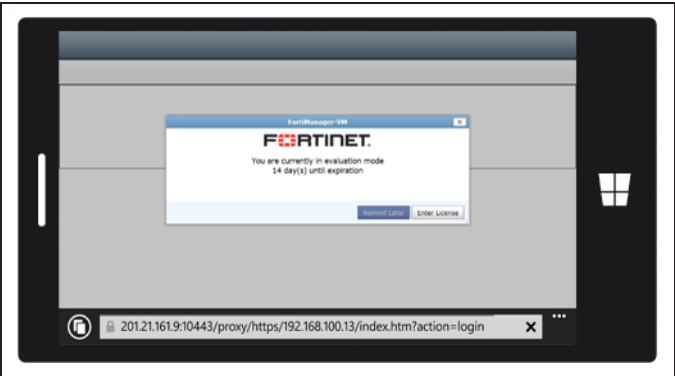
Log in using the credentials for your SSL VPN user.



After your credentials are accepted, you will be able to see the VPN portal.



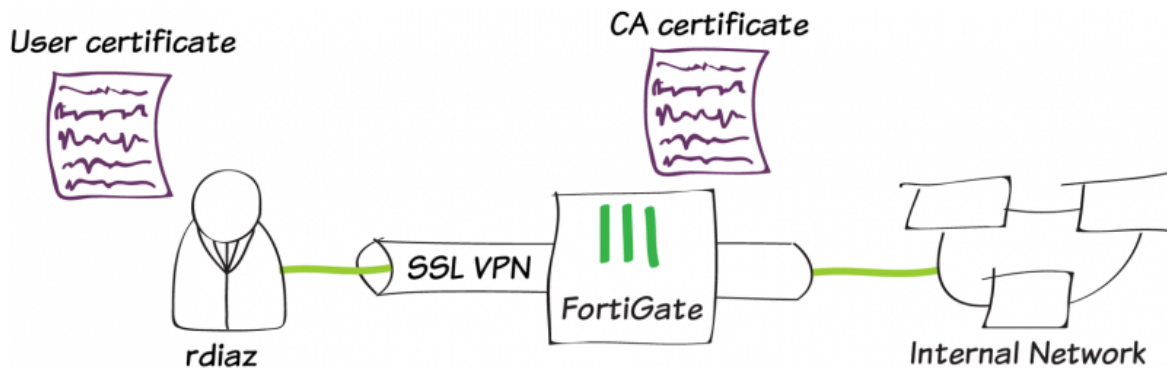
Select one of the pre-defined bookmarks (in the example, the bookmark for a FortiManager device). You will be able to access the network resource.



For further reading, check out [The SSL VPN web portal in the FortiOS 5.2 Handbook](#).



# SSL VPN with certificate authentication



In this recipe, you will configure an SSL VPN tunnel that requires users to authenticate using a certificate.

This recipe requires that you have three certificates:

- CA certificate
- server certificate (signed by the CA certificate)
- user certificate (signed by the CA certificate)

The certificates in the example were created using OpenSSL.

# 1. Enabling certificate management

Go to **System > Config > Features > Show More** and make sure that **Certificates** is enabled.

If necessary, **Apply** your changes.



# 2. Installing the server certificate

The server certificate is used for encrypting SSL VPN traffic and will be used for authentication.

Go to **System > Certificates** and select **Import > Local Certificate**.

Set **Type** to **Certificate**, choose the **Certificate file** and the **Key file** for your certificate, and enter the **Password**. If desired, you can also change the **Certificate Name**.

Import Certificate

Type

Certificate

Certificate file

Choose File

server.cert.pem

Key file

Choose File

server.key.pem

Password

.....

Certificate Name

Server\_Certificate

OK

Cancel

The server certificate now appears in the list of **Certificates**.

| Name                         | Subject  | Comments                           | Issuer                |
|------------------------------|--|------------------------------------|-----------------------|
| Local CA Certificates (1)    |  |                                    |                       |
| Fortinet_CA_SSLProxy         | C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority | This is the default CA certifi...  | Fortinet              |
| Certificates (5)             |  |                                    |                       |
| Fortinet_Factory             | C = US, CN = FG10003G12812324, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate         | This certificate is embedded in... | Fortinet              |
| Fortinet_Firmware            | C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate                | This certificate is embedded in... | Fortinet              |
| Fortinet_SSLProxy            | C = US, CN = FortiGate Server, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate         |                                    | Fortinet              |
| Fortinet_Wifi                | OU = PositiveSSL, CN = auth-cert.fortinet.com  | This certificate is embedded in... | Comodo CA Limited     |
| Server_Certificate           | C = CA, CN = vpn.fortinet.local, O = Fortinet, ST = Ontario, emailAddress = techdocs@fortinet.local, OU = Information Services           |                                    | Fortinet              |
| External CA Certificates (2) |  |                                    |                       |
| Fortinet_CA                  | C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority      |                                    | Fortinet              |
| PositiveSSL_CA               | CN = PositiveSSL CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester   |                                    | The USERTRUST Network |

### 3. Installing the CA certificate

The CA certificate is the certificate that signed both the server certificate and the user certificate. In this example, it is used to authenticate SSL VPN users.

Go to **System > Certificates** and select **Import > CA Certificate**.

Select **Local PC**, then select the certificate file.

Import CA Certificate

☐ SCEP

(URL of the SCEP server)

(Optional CA Identifier)

☒ Local PC

Browse...

ca.cert.pem

OK

Cancel

The CA certificate now appears in the list of **External CA Certificates** (in the example, it is called *CA\_Cert\_1*).

| Name                         | Subject  | Comments                           | Issuer                |
|------------------------------|--|------------------------------------|-----------------------|
| Local CA Certificates (1)    |  |                                    |                       |
| Fortinet_CA_SSLProxy         | C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority | This is the default CA certifi...  | Fortinet              |
| Certificates (5)             |  |                                    |                       |
| Fortinet_Factory             | C = US, CN = FG100D3G12812324, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate         | This certificate is embedded in... | Fortinet              |
| Fortinet_Firmware            | C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate                | This certificate is embedded in... | Fortinet              |
| Fortinet_SSLProxy            | C = US, CN = FortiGate Server, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate         |                                    | Fortinet              |
| Fortinet_Wifi                | OU = PositiveSSL, CN = auth-cert.fortinet.com  | This certificate is embedded in... | Comodo CA Limited     |
| Server_Certificate           | C = CA, CN = vpn.fortinet.local, O = Fortinet, ST = Ontario, emailAddress = techdocs@fortinet.local, OU = Information Services           |                                    | Fortinet              |
| External CA Certificates (3) |  |                                    |                       |
| CA_Cert_1                    | C = CA, CN = Fortinet Docs CA, L = Ottawa, O = Fortinet, ST = Ontario, emailAddress = techdocs@fortinet.local, OU = Information Services |                                    | Fortinet              |
| Fortinet_CA                  | C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority      |                                    | Fortinet              |
| PositiveSSL_CA               | CN = PositiveSSL CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester   |                                    | The USERTRUST Network |

### 4. Creating PKI users and a user group

In order to use certificate authentication, PKI users must be created in the CLI. Go to **System > Dashboard > Status** and enter the following commands into the CLI widget:

```
config user peer
    edit rdiaz
        set ca CA_Cert_1
        set subject User01
    end
```

Make sure that `subject` matches the name of the user certificate (in the example, *User01*)

Now that you have created a PKI user, a new menu has been added to the GUI. [tippy title="" class="myclass" showheader="false" width="auto" height="auto"]You may need to refresh the GUI before the menu appears.[/tippy] Go to **User & Device > PKI** to see the new user listed.

Edit the user account and expand **Two-factor authentication**. Enable **Require two-factor authentication** and set a **Password** for the account.

Go to **User & Device > User > User Groups** and create a group for SSL VPN users. Add the new user to the group.

Name

rdiaz

Subject

User01

CA

CA\_Cert\_1

Two-factor authentication

Require two-factor authentication

Password

Name

SSL-VPN-users

Type

Firewall

Fortinet Single Sign-On (FSSO)

Guest

RADIUS Single Sign-On (RSSO)

Members

rdiaz

## 5. Creating an SSL VPN portal

Go to **VPN > SSL > Portals**.

Edit the **full-access** portal. This portal supports both web and tunnel mode.

**Enable Split Tunneling** is *not* enabled so that all SSL VPN traffic will go through the FortiGate unit.

Name

full-access

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools

Click to add...

Client Options

☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

☒ Enable Web Mode

Portal Message

Welcome to SSL VPN Service

Theme

Blue

Page Layout

☒ Include Status Information

☒ Include Connection Tool

☒ Include FortiClient Download

☒ Prompt Mobile Users to Download FortiClient Application

☒ Include Login History

Number of History Entries

5

☒ Enable User Bookmarks

Predefined Bookmarks

Create New

Edit

Delete

| Name                      | Type | Location | Description |
|---------------------------|------|----------|-------------|
| No matching entries found |      |          |             |

☐ Limit Users to One SSL-VPN Connection at a Time

416

VPNs

## 6. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings**.

Under **Connection Settings**, set **Listen on Interface(s)** to **wan1**. To avoid conflicts, set **Listen on Port** to **10443**.

Set **Server Certificate** to the authentication certificate and enable **Require Client Certificate**.

Under **Authentication/Portal Mapping**, assign the user group to the **full-access** portal. If necessary, assign a portal for **All Other Users/Groups**.

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

*This is generally your external interface (i.e. wan1)*

Listen on Port

*Web mode access will be listening at <https://172.20.121.46:10443>*

Restrict Access ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout ☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For  (Seconds)

Server Certificate

Require Client Certificate ☒

**Tunnel Mode Client Settings**

Once connected in tunnel mode, clients will receive these settings.

Address Range ☒ Automatically assign addresses ☐ Specify custom IP ranges

*Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210*

DNS Server ☒ Same as client system DNS ☐ Specify

Specify WINS Servers ☐

Allow Endpoint Registration ☐

**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

| Users/Groups           | Portal      |
|------------------------|-------------|
| SSL-VPN-users          | full-access |
| All Other Users/Groups | full-access |

## 7. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**. Create a security policy allowing SSL VPN user to access the internal network.

Set **Incoming Interface** to **ssl.root**. Set **Source Address** to **all** and **Source User** to the new user group. Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.

Incoming Interface

Source Address

Source User(s)

Outgoing Interface

Destination Address

Schedule

Service

Action

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Add a second security policy allowing SSL VPN users to access the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

Make sure that **NAT** is enabled.

|   |  |     |
|---|--|-----|
| Incoming Interface  | ssl.root (SSL VPN interface)                 | +   |
| Source Address  | all  | +   |
| Source User(s)  | SSL-VPN-users                                | X + |
| Outgoing Interface  | wan1   | +   |
| Destination Address   | all  | +   |
| Schedule  | always                                       |     |
| Service   | ALL  | +   |
| Action  | ACCEPT                                       |     |
| <b>Firewall / Network Options</b>                               |  |     |
| <input checked="" type="checkbox"/> ON NAT                      |  |     |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port          |     |
| <input type="radio"/> Use Dynamic IP Pool                       | <input type="text" value="Click to add..."/> |     |

## 8. Installing the user certificate

To use the user certificate, it must first be installed on the user's PC. When the user attempts to authenticate, the user certificate will be checked against the CA certificate, to verify that they match.

Every user should have a unique user certificate, so that you can distinguish each user and so that it is possible to revoke a user's certificate if they should no longer have VPN access.

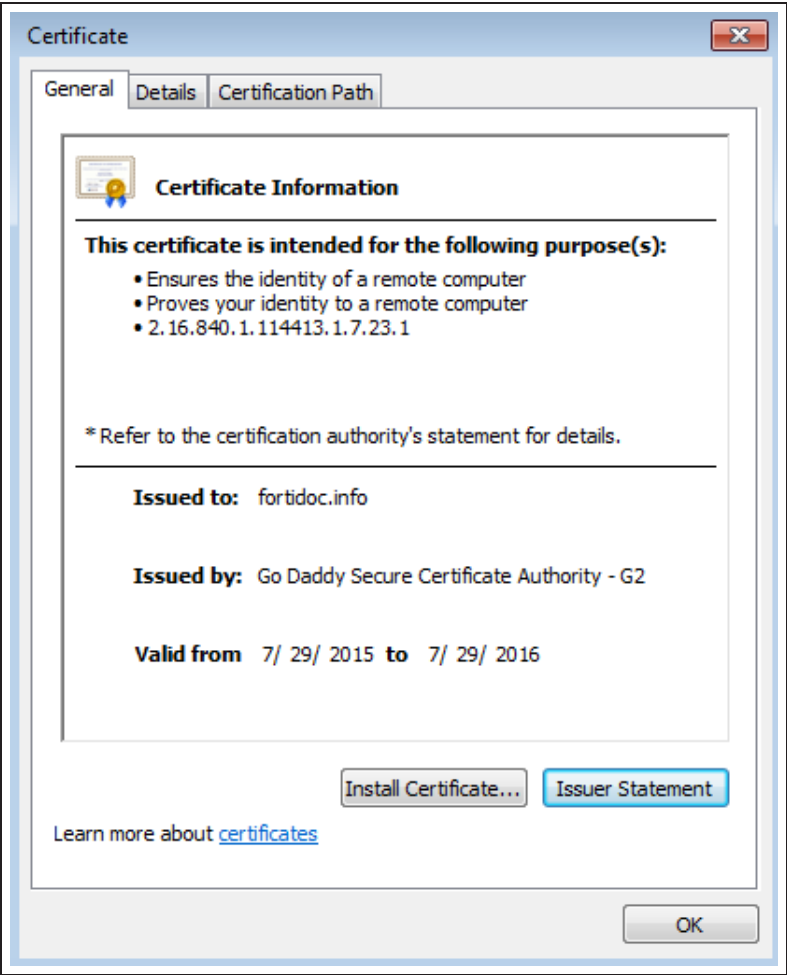
The installation instructions differ depending on what application is being used to connect to the VPN.

### Internet Explorer or Safari (on Windows or Mac OS):

If you are using the above applications to connect to the VPN, you must install the certificate into the certificate store for your OS. The certificate should be installed in the user's local certificate store (and not on the machine's local certificate store).

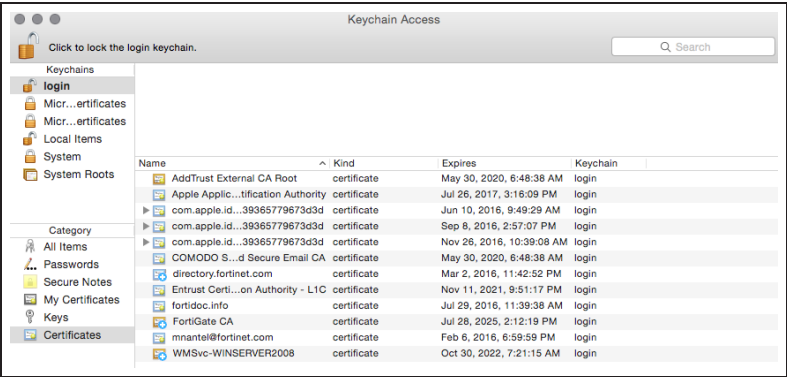
If you are using Windows 7/8/10, open the certificate file and select **Install Certificate**. The Import Wizard appears.

Import the certificate using the Import Wizard. Import the certificate into the **Personal** store.



If you are using Mac OS X, open the certificate file. **Keychain Access** opens.

Double-click the certificate. Expand **Trust** and select **Always Trust**.



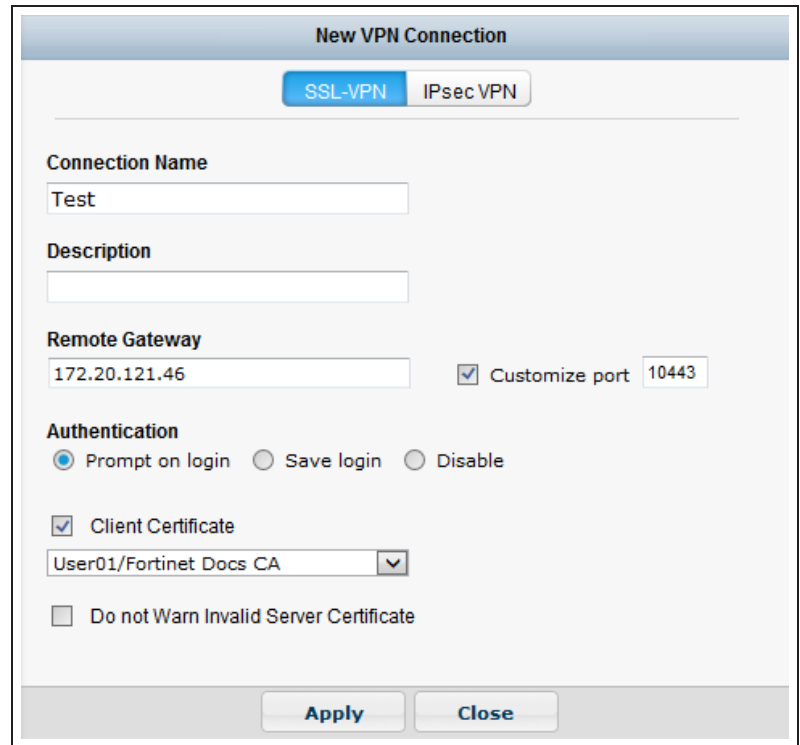


## FortiClient (on Windows or Mac OS)

In order to connect to the VPN with FortiClient, you will first have to use the above instructions to install the certificate for your OS. Once the certificate has been installed, you can configure FortiClient to access the VPN.

Open **FortiClient** and go to **Remote Access > Configure VPN**. Create a new **SSL VPN** connection.

Set the **Connection Name**, **Remote Gateway**, and **Customize port**. Enable **Client Certificate** and select the authentication certificate.



The screenshot shows the 'New VPN Connection' dialog box in FortiClient. It has two tabs: 'SSL-VPN' (selected) and 'IPsec VPN'. The fields are as follows:

- Connection Name:** Text box containing 'Test'.
- Description:** Empty text box.
- Remote Gateway:** Text box containing '172.20.121.46'.
- Customize port:** A checked checkbox followed by a text box containing '10443'.
- Authentication:** Three radio buttons: 'Prompt on login' (selected), 'Save login', and 'Disable'.
- Client Certificate:** A checked checkbox followed by a dropdown menu showing 'User01/Fortinet Docs CA'.
- Do not Warn Invalid Server Certificate:** An unchecked checkbox.

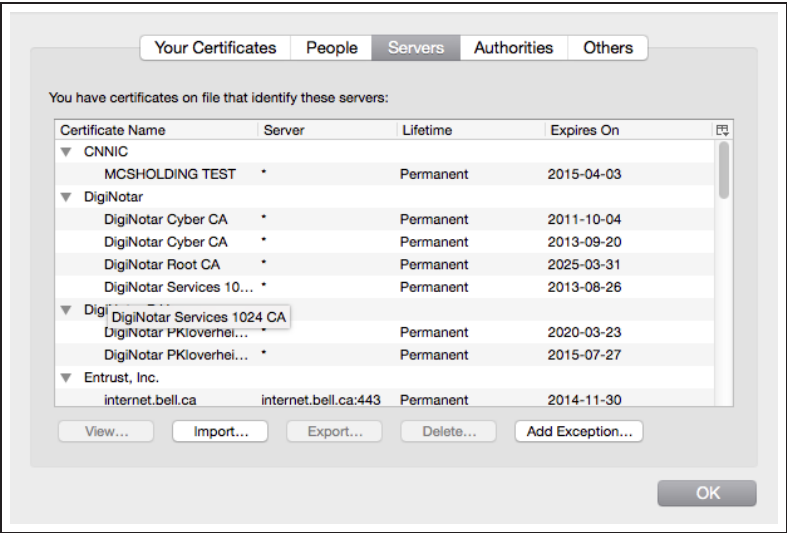
At the bottom are 'Apply' and 'Close' buttons.

## Firefox (on Windows or Mac OS)

Firefox has its own certificate store. If you will be using Firefox to connect to the VPN, then the user certificate must be installed in this store, rather than in the OS.

Depending on the version, go to **Menu > Options** or **Preferences > Advanced** and find the **Certificates** tab.

Select **View Certificates**, then select the **Your Certificates** list. **Import** the certificate file.



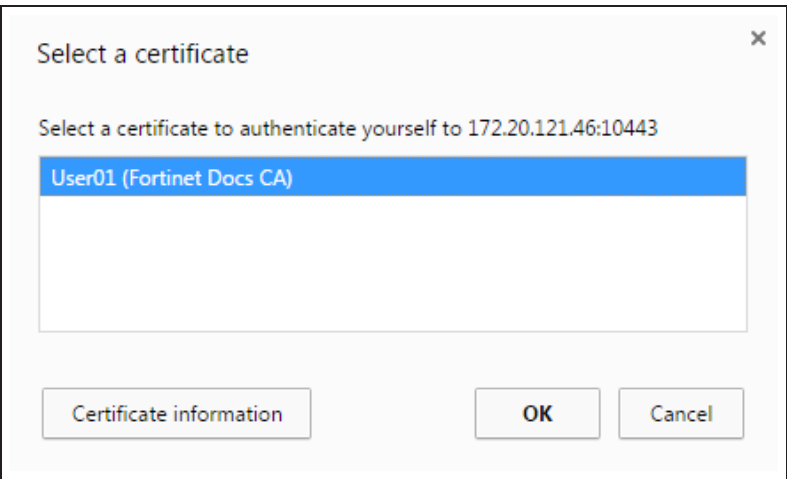
## 9. Results

### Using a web browser

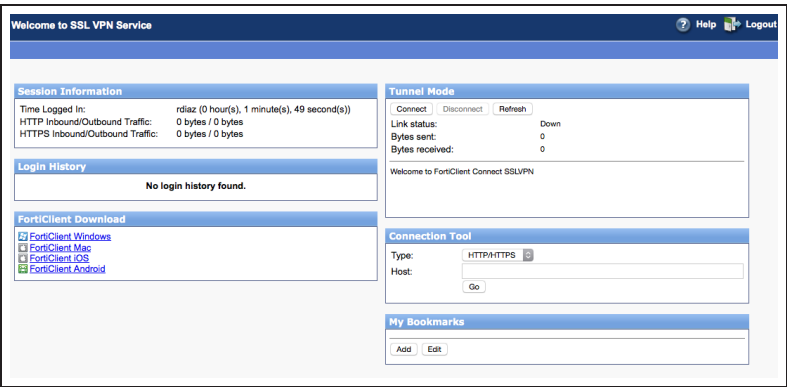
Browse to the SSL VPN portal (in the example, *http://172.20.121.46:10443*).

A message will appear requesting a certificate for authentication. Select the user certificate.

Enter your user credentials when requested.

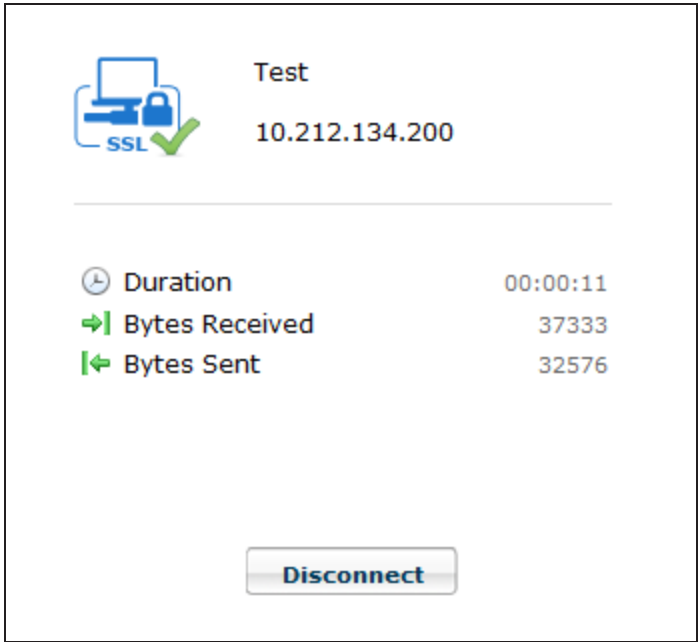


You are able to connect to the SSL VPN web portal.



Using FortiClient

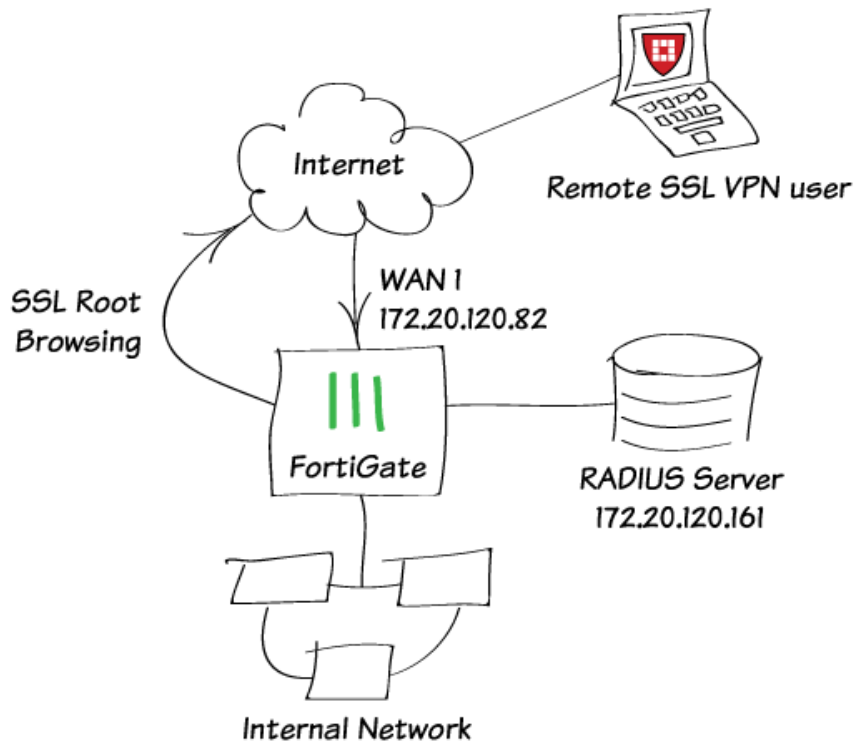
Open FortiClient and connect to the VPN. You are able to connect.



On the FortiGate, go to VPN > Monitor > SSL-VPN Monitor. You can see that the user is currently connected to the VPN.

|                          | No. | User  | Source IP    | Begin Time               |
|--------------------------|-----|-------|--------------|--------------------------|
| <input type="checkbox"/> | 1   | rdiaz | 172.25.162.2 | Fri Sep 25 13:39:46 2015 |

# SSL VPN with RADIUS authentication



This recipe provides remote FortiClient users with access to the corporate network using SSL VPN and Internet browsing through the corporate FortiGate unit. Remote users are authenticated using RADIUS (configured in Microsoft's Network Policy Server).

FortiClient is available [here](#).

The recipe includes a brief explanation of the RADIUS server configuration we utilized. It was tested on a FortiGate 60D. Microsoft Network Policy Server was configured on Windows Server 2008.

## 1. Configuring Microsoft's Network Policy Server

In RADIUS Client properties, enable the client and set **Vendor name** to **RADIUS Standard**.

Uncheck both **Access-Request message must contain the Message-Authenticator attribute** and **RADIUS client is NAP-capable**.

**FortiGate\_Testing\_SSL Properties**

Settings

☒ Enable this RADIUS client

Friendly name:  
FortiGate\_Testing\_SSL

Address (IP or DNS):  
172.20.120.82 Verify...

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret: .....

Confirm shared secret: .....

☐ Access-Request messages must contain the Message-Authenticator attribute

☐ RADIUS client is NAP-capable

OK Cancel Apply

**Network Policy Server**

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
  - RADIUS Clients**
  - Remote RADIUS Server Groups
- Policies
  - Connection Request Policies
  - Network Policies
  - Health Policies
- Network Access Protection
- Accounting

RADIUS clients allow you to specify the network access servers, that provide access to your network.

| Friendly Name         | IP Address    | Device Manufacturer | NAP-Capable | Status  |
|-----------------------|---------------|---------------------|-------------|---------|
| FortiGate_Testing_SSL | 172.20.120.82 | RADIUS Standard     | No          | Enabled |

In **Connection Request Properties > Overview**, create a policy, name it and enable it.

Set **Type of network access server** to **Unspecified**.

The screenshot shows the 'SSL\_Connection\_Request Properties' dialog box with the 'Overview' tab selected. The 'Policy name' field is set to 'SSL\_Connection\_Request'. The 'Policy State' section has 'Policy enabled' checked. The 'Network connection method' section has 'Type of network access server' set to 'Unspecified'.

SSL\_Connection\_Request Properties

Overview | Conditions | Settings

Policy name: SSL\_Connection\_Request

Policy State  
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Network connection method  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:  
Unspecified

☐ Vendor specific:  
10

OK Cancel Apply

In **Connection Request Properties > Conditions**, set the **Condition** to either **NAS Identifier** (the FortiGate Name) or **NAS IPv4 Address** (the FortiGate IP).

You can also configure both. Just be aware that if there is more than one condition configured, they must all pass to allow the connection.

The screenshot shows the 'SSL\_Connection\_Request Properties' dialog box with the 'Conditions' tab selected. A table lists one condition: 'NAS IPv4 Address' with the value '172.20.120.82'. The 'Add...' button is highlighted with a red box.

SSL\_Connection\_Request Properties

Overview | Conditions | Settings

Configure the conditions for this network policy.

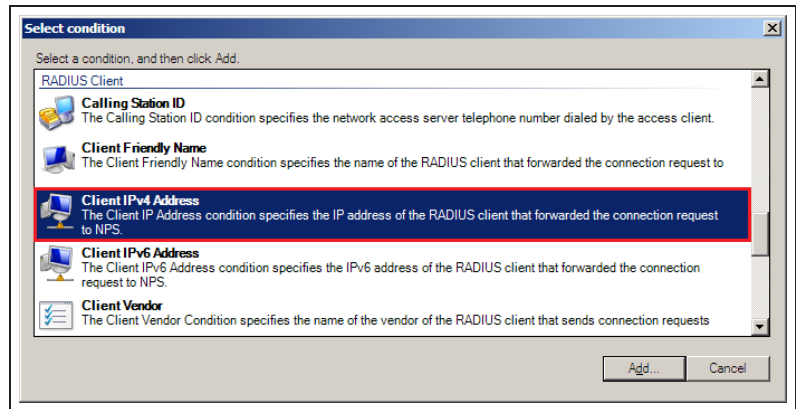
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

| Condition        | Value         |
|------------------|---------------|
| NAS IPv4 Address | 172.20.120.82 |

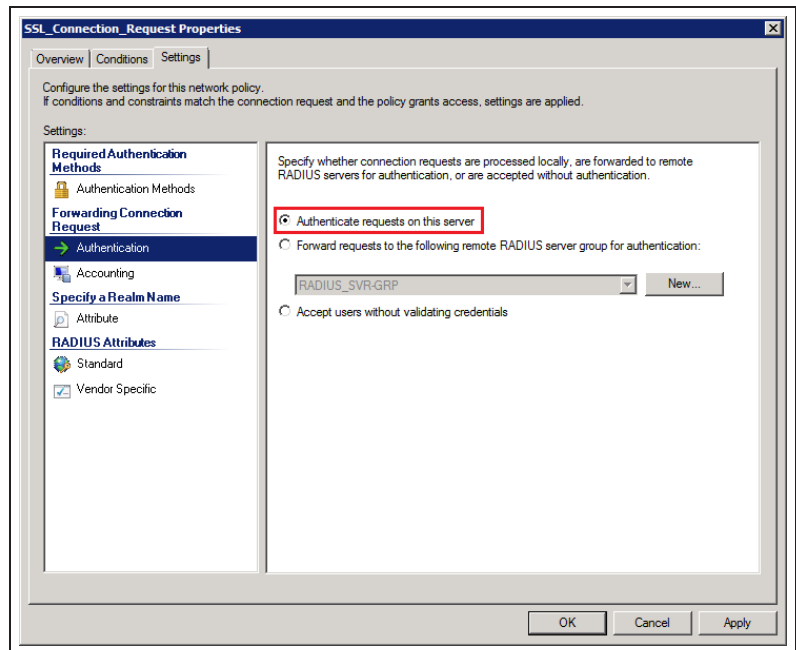
Condition description:  
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

Add... Edit... Remove

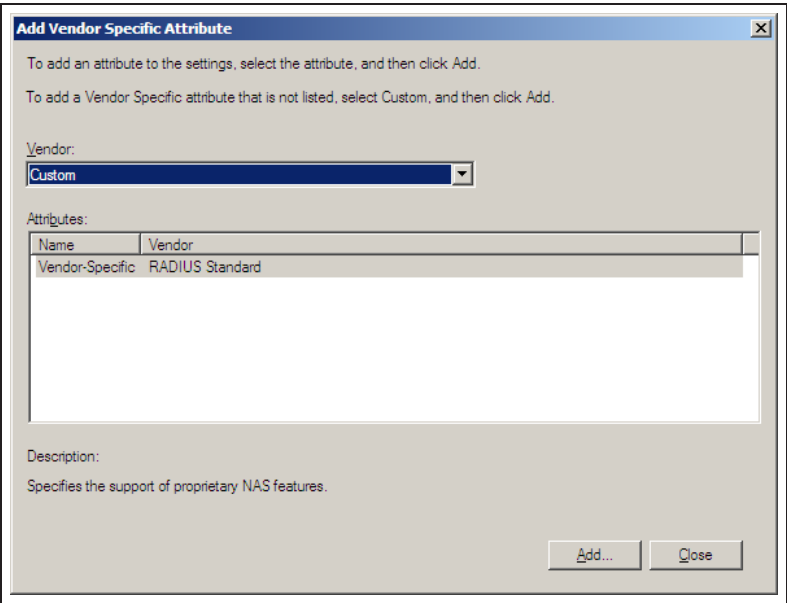
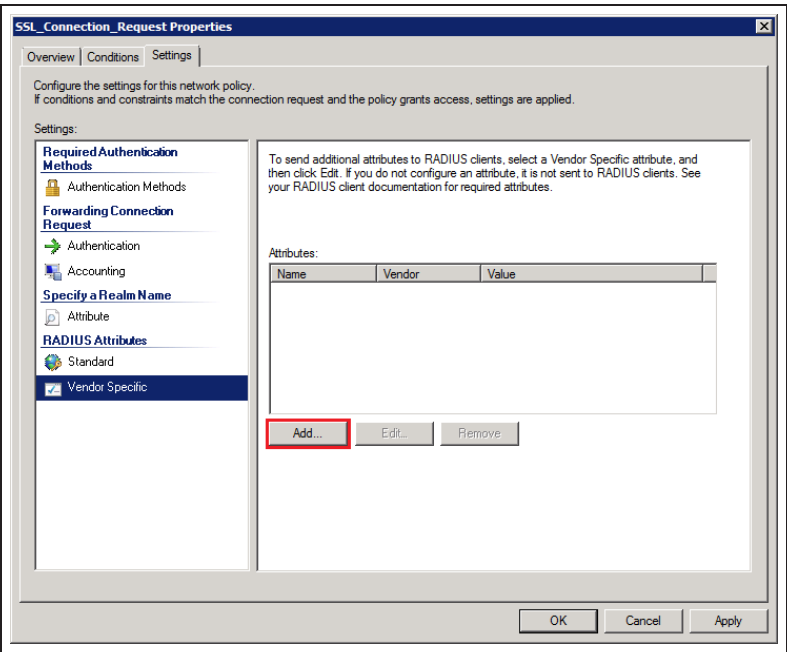
OK Cancel Apply



In Connection Request Properties > Settings > Authentication, make sure **Authenticate requests on this server** is enabled.



In **Connection Request Properties > Vendor Specific**, add a new **Vendor-Specific** attribute with **Vendor** set to **RADIUS Standard** and the **Vendor Code 12356**.





In **Network Policies > Overview**, create a policy, name it and enable it.

Set **Type of network access server** to **Unspecified**.

The screenshot shows the 'SSL Authentication Properties' dialog box with the 'Overview' tab selected. The 'Policy name' field is set to 'SSL Authentication'. The 'Policy State' section has 'Policy enabled' checked. The 'Access Permission' section has 'Grant access' selected. The 'Network connection method' section has 'Type of network access server' selected, and the dropdown menu shows 'Unspecified'.

**SSL Authentication Properties**

Overview | Conditions | Constraints | Settings

Policy name: **SSL Authentication**

☐ Policy State  
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

**Access Permission**  
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.

☐ Deny access. Deny access if the connection request matches this policy.

☐ Ignore user account dial-in properties.  
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:  
**Unspecified**

☐ Vendor specific:  
10

OK Cancel Apply

In **Network Policies > Conditions**, add a User Group that contains the users you want to allow connection to the VPN and apply the necessary conditions.

The screenshot shows the 'SSL Authentication Properties' dialog box with the 'Conditions' tab selected. The 'Condition' list is empty. The 'Add...' button is highlighted with a red box. The 'Condition description' text at the bottom explains that the Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

**SSL Authentication Properties**

Overview | **Conditions** | Constraints | Settings

Configure the conditions for this network policy.

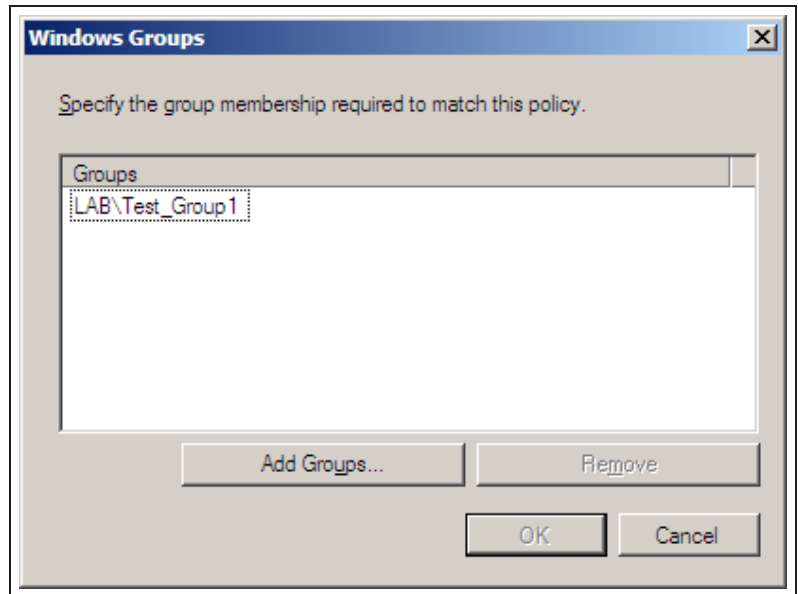
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

| Condition | Value |
|-----------|-------|
|-----------|-------|

Condition description:  
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

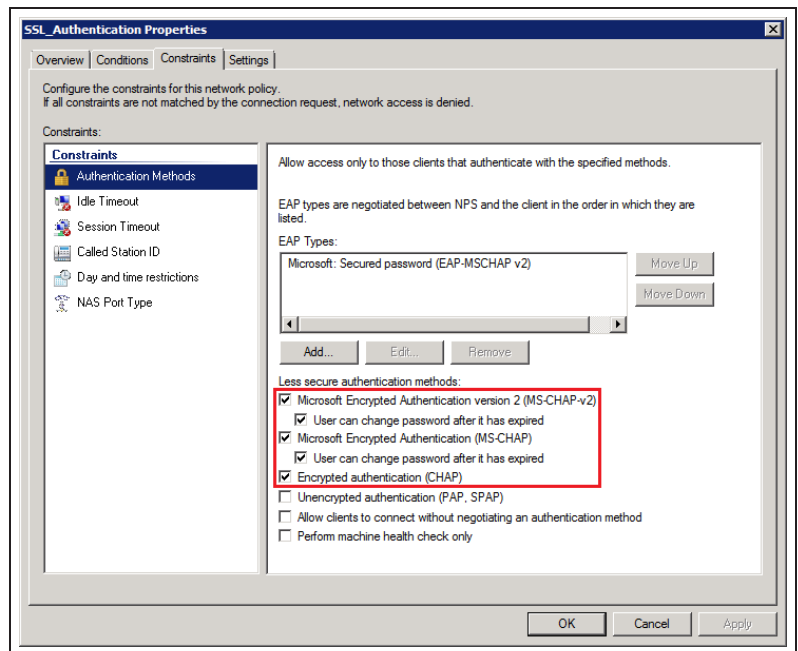
**Add...** Edit... Remove

OK Cancel Apply



In **Network Policies > Constraints > Authentication Methods**, enable **MS-CHAP-v2**.

You do not need to modify any of the remaining network policy settings.



## 2. Configuring the FortiGate to connect to the RADIUS server

On your FortiGate, go to **User & Device > Authentication > RADIUS Servers**.

Enter a **Name** for the RADIUS server, and enter its **Primary Server IP/Name**.

Carefully and correctly enter the **Primary Server Secret**, and specify the authentication method **MS-CHAP-v2**.

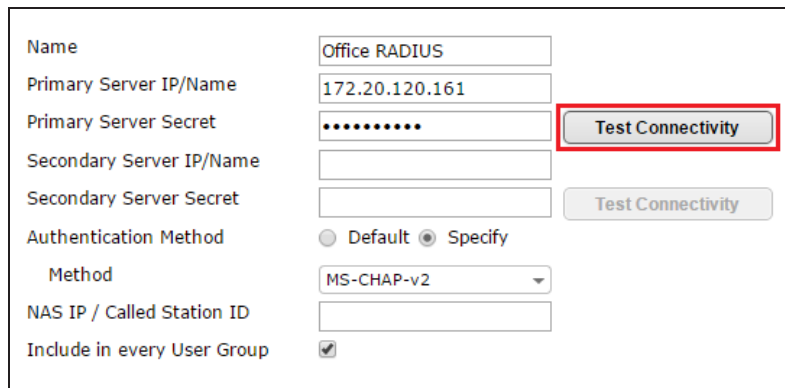
Perform a RADIUS connectivity test by clicking **Test Connectivity**.

Enter valid RADIUS credentials and click **Test**.

If there is an error in the configuration, or the credentials were entered incorrectly, the RADIUS connectivity test returns with a **Server is unreachable** error. If this occurs, double-check the configuration for errors and try again.

If everything is configured and entered correctly, the RADIUS connectivity test returns with a **Successful** confirmation message.

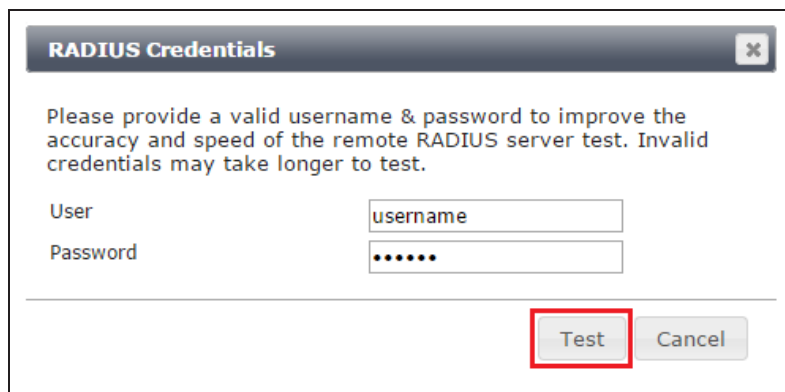
Click **OK**.



|                             |  |
|-----------------------------|--|
| Name                        | Office RADIUS  |
| Primary Server IP/Name      | 172.20.120.161   |
| Primary Server Secret       | .....  |
| Secondary Server IP/Name    |  |
| Secondary Server Secret     |  |
| Authentication Method       | <input type="radio"/> Default <input checked="" type="radio"/> Specify |
| Method                      | MS-CHAP-v2   |
| NAS IP / Called Station ID  |  |
| Include in every User Group | <input checked="" type="checkbox"/>                                    |

Test Connectivity

Test Connectivity



**RADIUS Credentials**

Please provide a valid username & password to improve the accuracy and speed of the remote RADIUS server test. Invalid credentials may take longer to test.

User: username

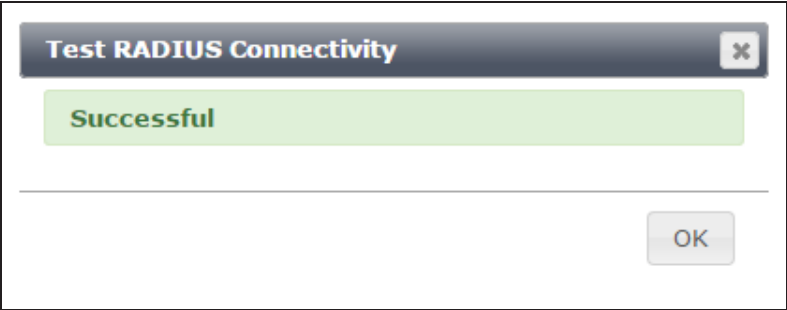
Password: .....

Test Cancel



**Test RADIUS Connectivity**

OK

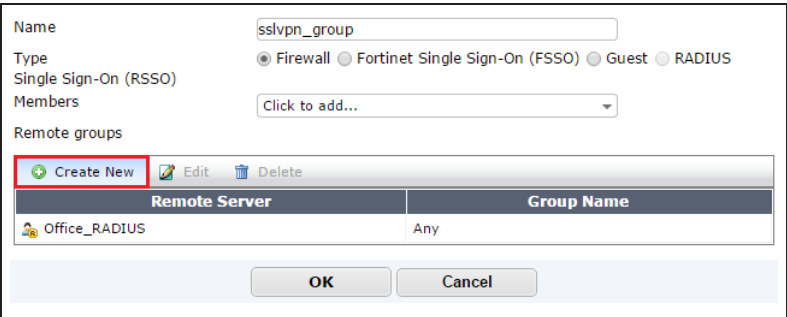


### 3. Adding the SSL VPN remote user group

Go to **User & Device > User > User Groups**.

Create an SSL VPN remote user group and add the RADIUS server as a **Remote group**.

You can choose to specify a group name that matches a group in the RADIUS configuration, or leave it set to **Any** (the default setting), which permits any user configured on the RADIUS server.



## 4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Portals**.

Edit the **full-access** portal.

**Enable Split Tunneling** is *not* enabled so that all SSL VPN traffic will go through the FortiGate unit.

Create New

Edit

Delete

| Name          | Tunnel Mode | Web Mode | Ref. |  |
|---------------|-------------|----------|------|--|
| full-access   | ✓           | ✓        | 2    |  |
| tunnel-access | ✓           | ✗        | 0    |  |
| web-access    | ✗           | ✓        | 0    |  |

Name: full-access

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools: SSLVPN\_TUNNEL\_ADDR1

Client Options: ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **10443**.

Disable **Require Client Certificate**.

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s): wan1

Listen on Port: 10443

Restrict Access: ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout: ☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For: 300 (Seconds)

Server Certificate: Fortinet\_CA\_SSLProxy

Require Client Certificate: ☐

## 5. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing SSL VPN user to access the internal network.

Set **Incoming Interface** to **ssl.root**. Set **Source Address** to **all** and **Source User** to the remote user group. Set **Outgoing Interface** to the local network interface so that the remote user(s) can access the internal network.

Set **Destination Address** to all, enable **NAT**, and configure any remaining firewall and security options as desired.

Incoming Interface: ssl.root (SSL VPN interface)

Source Address: SSLVPN\_TUNNEL\_ADDR1

Source User(s): sslvpn\_group

Outgoing Interface: internal1 (Local LAN)

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Add a second security policy allowing SSL VPN users to access the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

Set **Source User** to the remote user group.

|   |  |
|---|--|
| Incoming Interface  | ssl.root (SSL VPN interface)                 |
| Source Address  | SSLVPN_TUNNEL_ADDR1                          |
| Source User(s)  | sslvpn_group                                 |
| Outgoing Interface  | wan1   |
| Destination Address   | all  |
| Schedule  | always                                       |
| Service   | ALL  |
| Action  | ACCEPT                                       |
| <b>Firewall / Network Options</b>                               |  |
| <input checked="" type="checkbox"/> NAT                         |  |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port          |
| <input type="radio"/> Use Dynamic IP Pool                       | <input type="text" value="Click to add..."/> |

## 6. Configuring FortiClient

Open FortiClient, go to **Remote Access**, and add a new SSL VPN connection.

Antivirus  
Real-time Protection Disabled

Parental Control  
4 Violations

Remote Access  
No VPN Connected

Password

Add a new connection

Edit the selected connection

Delete the selected connection

Provide a **Connection Name** and set the **Type** to SSL VPN.

Set **Remote Gateway** to the FortiGate **IP address**.

Set **Customize Port** to **10443**.

Edit VPN Connection

Connection Name

FortiGate\_with\_SSL

Type

SSL-VPN

IPsec VPN

Description

FortiGate\_with\_SSL

Remote Gateway

172.20.120.82

☒

Customize port

10443

Authentication

☐ Prompt on login

☒ Save login

Username

twhite

Client Certificate

☐

Do not Warn Invalid Server Certificate

☐

OK

Cancel

Delete

Select the new connection, enter a valid username and password, and click **Connect**.

AntiVirus  
Real-time Protection Disabled

Parental Control  
4 Violations

Remote Access  
No VPN Connected

FortiGate\_with\_SSL

twhite

Password

If prompted with a server authentication warning, select **Yes**.

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Yes

No

View Certificate

More Info

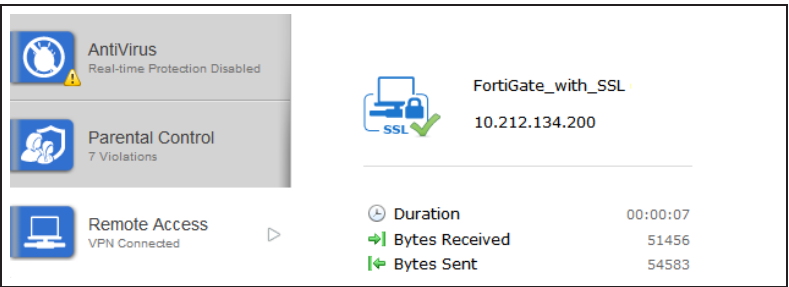
## 7. Results

VPNs

434

From FortiClient start an SSL VPN session. As the connection is being established, the FortiGate authenticates the user against the RADIUS server and, if successful, assigns the user an IP address.

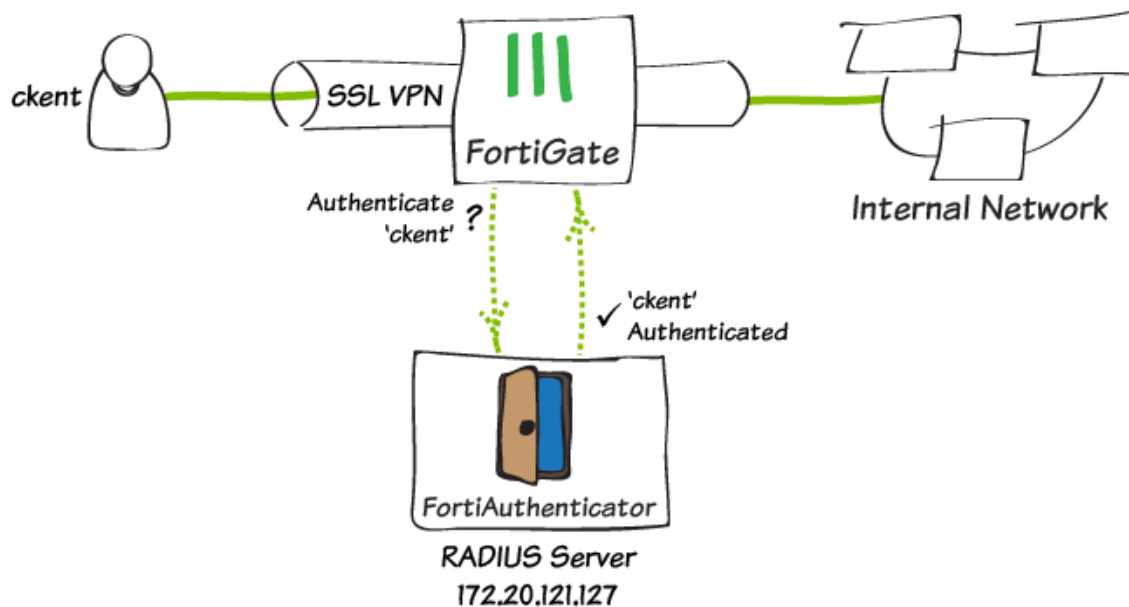
FortiClient then displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



For further reading, check out [Basic SSL VPN configuration](#) in the [FortiOS 5.2 Handbook](#).



# RADIUS authentication for SSL VPN with FortiAuthenticator



This recipe describes how to set up FortiAuthenticator to function as a RADIUS server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the RADIUS client on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as a RADIUS server.

A video of this recipe is available [here](#).

## 1. Create the User(s) on FortiAuthenticator

From the FortiAuthenticator GUI, go to **Authentication > User Management > Local Users**, and select **Create New**.

Enter a name for the user (in the example, *ckent*), enter and confirm a password, and select **OK**. Select **OK** again to bypass optional settings.

The screenshot shows the 'Create New' user form in the FortiAuthenticator GUI. The 'Username' field is populated with 'ckent'. Below it, there are checkboxes for 'Disabled', 'Password-based authentication' (checked), 'Token-based authentication', 'Allow RADIUS authentication' (checked), and 'Enable account expiration'. The 'User Role' section has radio buttons for 'Administrator' and 'User' (selected). There is also a checkbox for 'Allow LDAP browsing'. Below these are several expandable sections: 'User Information', 'Alternative Email Addresses', 'Password Recovery Options', 'Groups', 'Email Routing', 'RADIUS Attributes', and 'Certificate Bindings'. At the bottom are 'OK' and 'Cancel' buttons.

Next, go to **Authentication > User Management > User Groups**, and add a user group for the FortiGate users. Add the desired users to the group.

The screenshot shows the 'Add Users' dialog in the FortiAuthenticator GUI. The 'Name' field is set to 'Local'. The 'Type' section has radio buttons for 'Local' (selected), 'Remote LDAP', and 'Remote RADIUS'. The 'Users' section contains two lists: 'Available users' and 'Selected users'. The 'Available users' list has a search filter and shows 'bwayne' and 'jgarlick'. The 'Selected users' list shows 'abristow' and 'ckent'. At the bottom are 'Choose all visible' and 'Remove all' buttons.

## 2. Create the RADIUS Client on FortiAuthenticator

Go to **Authentication > RADIUS Service > Clients**, and select **Create New**.

Enter a name for the RADIUS Client, set **Client name/IP** to the IP of the FortiGate, and set a **Secret**. The Secret is a pre-shared, secure password that the FortiGate will use to authenticate to the FortiAuthenticator.

Be sure to set **Authentication method** to **Password-only authentication (exclude users without a password)**, and set **Realms** to **local | Local users**.

The screenshot shows the 'Create New' form for a RADIUS Client. The fields are: Name: RADIUSclient, Client name/IP: 172.20.121.56, and Secret: a masked password field with eight dots.

The screenshot shows the 'Authentication method' and 'Realms' configuration. Under 'Authentication method', 'Password-only authentication (exclude users without a password)' is selected. Under 'Username input format', 'username@realm' is selected. The 'Realms' table shows a single realm: 'local | Local users'.

| Default                          | Realm               | Allow local users to override remote users | Use Windows AD domain authentication | Groups                                       | Delete                   |
|----------------------------------|---------------------|--|--------------------------------------|--|--------------------------|
| <input checked="" type="radio"/> | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | Filter: [Edit]<br>Filter local users: [Edit] | <input type="checkbox"/> |

## 3. Connect the FortiGate to the RADIUS Server

From the FortiGate GUI, go to **User & Device > Authentication > RADIUS Servers**, and select **Create New**.

Enter a name for the RADIUS server, enter the IP address of the FortiAuthenticator, and enter the **Secret** created before.

Test the connectivity and enter the credentials for 'ckent'. The test should come back with a successful connection.

The screenshot shows the 'Create New' form for a RADIUS Server. The fields are: Name: FAC-RADIUS, Primary Server IP/Name: 172.20.121.127, Primary Server Secret: a masked password field, Secondary Server IP/Name: (empty), Secondary Server Secret: (empty), Authentication Method: Default (selected), NAS IP / Called Station ID: (empty), and Include in every User Group: (unchecked). Below the form is a 'Test RADIUS Connectivity' dialog box showing 'Successful'.

## 4. Create the RADIUS User Group on the FortiGate

Go to **User & Device > User > User Groups**, and select **Create New**.

Enter a name for the user group, and under **Remote Groups**, select **Create New**.

Name: RADIUSgroup

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: Click to add...

Remote groups

Create New Edit Delete

| Remote Server             | Group Name |
|---------------------------|------------|
| No matching entries found |            |

Select **FAC-RADIUS** under the **Remote Server** dropdown.

Add Group Match

Remote Server: Please Select

Groups: LDAP, LDAPserver, RADIUS, FAC-RADIUS

OK Cancel

**FAC-RADIUS** has been added to the RADIUS group.

Name: RADIUSgroup

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: Click to add...

Remote groups

Create New Edit Delete

| Remote Server | Group Name |
|---------------|------------|
| FAC-RADIUS    | Any        |

## 5. Configure the SSL VPN

From the FortiGate GUI, go to **VPN > SSL > Portals**, and edit the **full-access** portal.

Disable **Split Tunneling**.

Name: full-access

☒ Enable Tunnel Mode

☐ **Enable Split Tunneling**

Source IP Pools: SSLVPN\_TUNNEL\_ADDR1

☒ Enable IPv6 Tunnel Mode

☒ Enable IPv6 Split Tunneling

IPv6 Routing Address: Click to add...

Source IPv6 Pools: SSLVPN\_TUNNEL\_IPv6\_ADE

Client Options: ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

Go to **VPN > SSL > Settings**.

Under **Connection Settings** set **Listen on Port** to **10443**.

Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges** and set it to **SSLVPN\_TUNNEL\_ADDR1**.

Under **Authentication/Portal Mapping**, select **Create New**.

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s): wan1

Listen on Port: 10443

Restrict Access: ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout: ☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For: 300 (Seconds)

Server Certificate: Fortinet\_Factory

Require Client Certificate: ☐

**Tunnel Mode Client Settings**

Once connected in tunnel mode, clients will receive these settings.

Address Range: ☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges: SSLVPN\_TUNNEL\_ADDR1

DNS Server: ☒ Same as client system DNS ☐ Specify

Specify WINS Servers: ☐

Allow Endpoint Registration: ☐

**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

**Create New** **Edit** **Delete**

| Users/Groups           | Realm | Portal     |
|------------------------|-------|------------|
| All Other Users/Groups | /     | web-access |

Assign the **RADIUSgroup** user group to the full-access portal, and assign **All Other Users/Groups** to the desired portal.

**Create New** **Edit** **Delete**

| Users/Groups           | Realm | Portal      |
|------------------------|-------|-------------|
| RADIUSgroup            | /     | full-access |
| All Other Users/Groups | /     | full-access |

Select the prompt at the top of the screen to create a new SSL-VPN policy.

Set **Source User(s)** to the **RADIUSgroup** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

Incoming Interface

ssl.root (SSL VPN interface)

Source Address

all

Source User(s)

RADIUSgroup

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON NAT

6. Results

From a remote device, access the SSL VPN Web Portal.

Enter valid RADIUS credentials (in the example, *ckent*).

Please Login

Name:

ckent

Password:

.....

Login

'ckent' is now successfully logged into the SSL VPN Portal.

Welcome to SSL VPN Service

Session Information

Time Logged In:

ckent (0 hour(s), 0 minute(s), 0 second(s))

HTTP Inbound/Outbound Traffic:

0 bytes / 0 bytes

HTTPS Inbound/Outbound Traffic:

0 bytes / 0 bytes

Login History

| Time                   | Time Logged In       | Inbound/Outbound Traffic |
|------------------------|----------------------|--------------------------|
| 8/14/2015, 11:22:11 AM | 5 Minutes 2 Seconds  | 0 B / 0 B                |
| 8/13/2015, 5:29:04 PM  | 5 Minutes 1 Seconds  | 0 B / 0 B                |
| 8/13/2015, 4:00:12 PM  | 9 Minutes 23 Seconds | 0 B / 0 B                |

FortiClient Download

FortiClient Windows

FortiClient Mac

FortiClient iOS

FortiClient Android

Tunnel Mode

The Fortinet SSL-VPN Client plugin is not installed on your computer, is not up to date, or your browser settings are blocking the plugin from running. The plugin is required for the tunnel mode function of the SSL-VPN Client.

You need to have administrator rights to perform the first time installation. Once it is installed, it runs under normal user privileges and can be upgraded to newer versions without administrator privileges.

Connection Tool

Type:

HTTP/HTTPS

Host:

Go

My Bookmarks

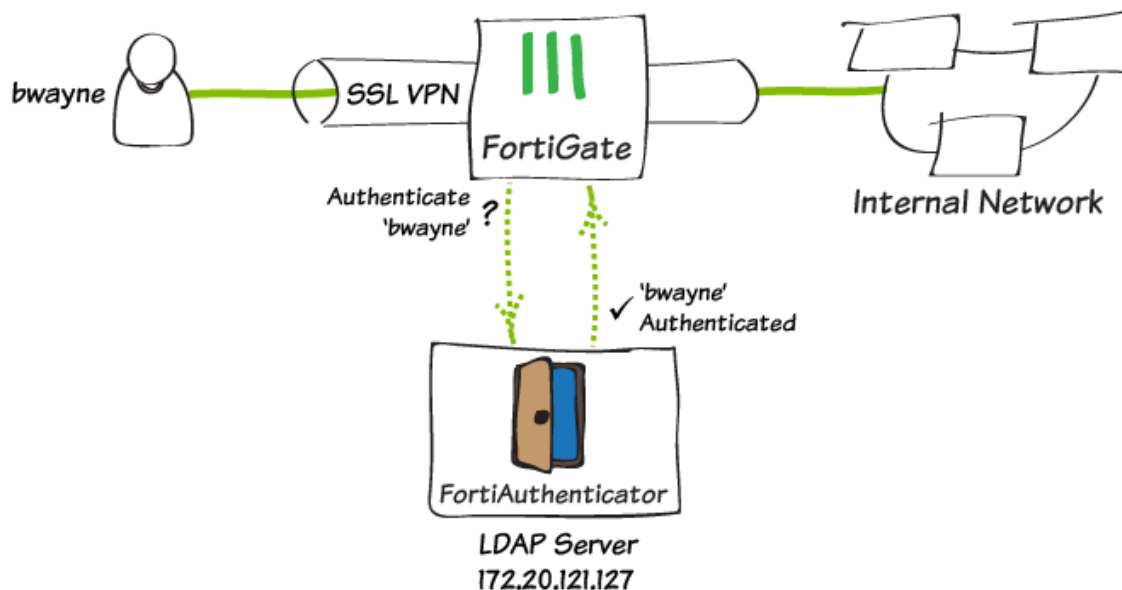
Add

Edit

From the FortiGate GUI, go to **VPN > Monitor > SSL-VPN Monitor** to confirm the connection.

|                                     | No. | User  | Source IP     | Begin Time               | Description |
|-------------------------------------|-----|-------|---------------|--------------------------|-------------|
| <input checked="" type="checkbox"/> | 1   | ckent | 172.20.120.91 | Fri Aug 14 09:15:40 2015 |             |

# LDAP authentication for SSL VPN with FortiAuthenticator



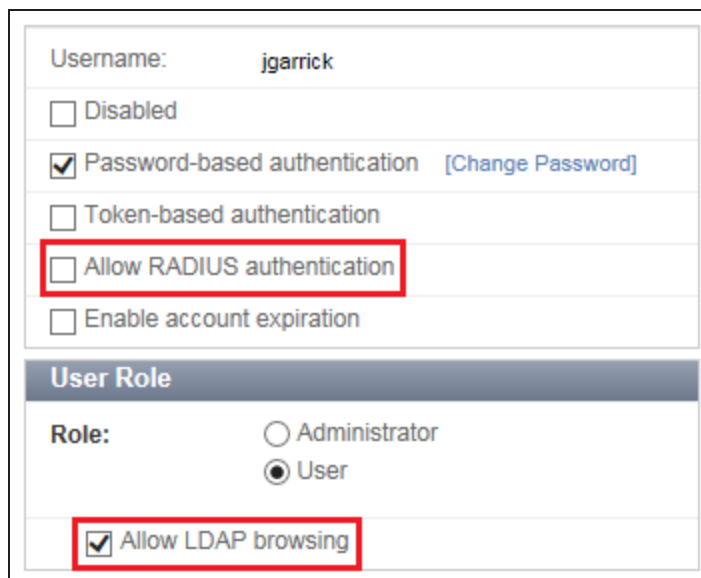
This recipe describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an LDAP server.

## 1. Create the User and User Group on FortiAuthenticator

From the FortiAuthenticator GUI, go to **Authentication > User Management > Local Users**, and select **Create New**.

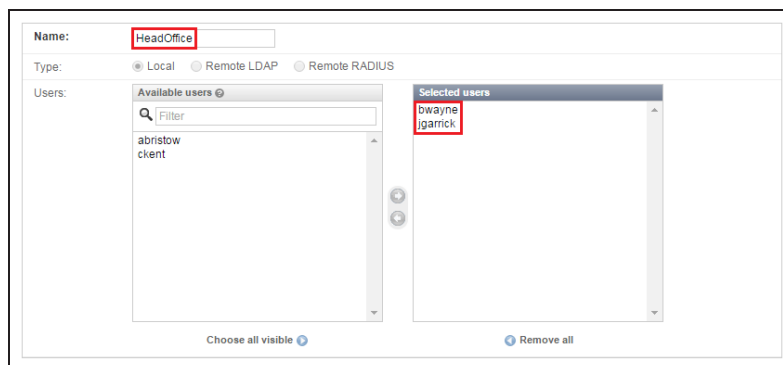
Enter a name for the user (in the example, *jgarrick*), enter and confirm a password, and be sure to *disable* **Allow RADIUS authentication** – RADIUS authentication is not required for this recipe.

Set **Role** as **User**, and select **OK**. New options will appear.



Make sure to enable **Allow LDAP browsing** – the user will not be able to connect to the FortiGate otherwise.

Next, go to **Authentication > User Management > User Groups**, and add a user group for the FortiGate users. Add the desired users to the group.



## 2. Create the LDAP Directory Tree on FortiAuthenticator

Go to **Authentication > LDAP Service > Directory Tree**, and create a Distinguished Name (DN) (in the example, *dc=fortinet,dc=com*). A DN is made up of Domain Components (DC).

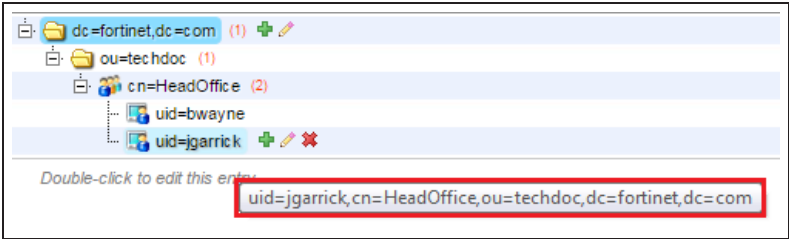


Both the users and the user group created earlier are the User ID (UID) and the Common Name (CN) in the LDAP Directory Tree.

Create an Organizational Unit (OU), and a Common Name (CN). Under the **cn=HeadOffice** entry, add UIDs for each user.

If you mouse over one of the users, you will see the full DN of the LDAP server.

Later, you will use **kgarrick** on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use **bwayne** credentials to connect to the VPN tunnel.



### 3. Connect the FortiGate to the LDAP Server

From the FortiGate GUI, go to **User & Device > Authentication > LDAP Servers**, and select **Create New**.

Enter a name for the LDAP Server connection.

Set **Server IP/Name** as the IP of the FortiAuthenticator, and set the Common Name Identifier as **uid**.

|                        |                |
|------------------------|----------------|
| Name                   | LDAPserver     |
| Server IP/Name         | 172.20.121.127 |
| Server Port            | 389            |
| Common Name Identifier | uid            |

Set the **Distinguished Name** as **dc=fortinet,dc=com**, and set the **Bind Type** to **Regular**.

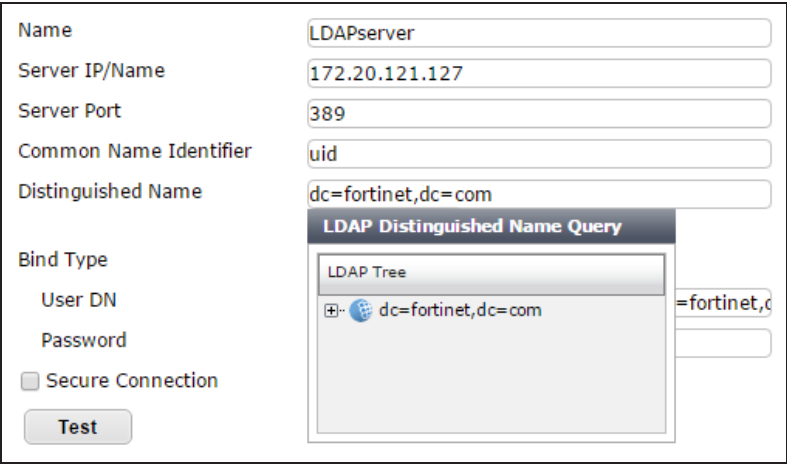
Next, enter the **User DN** of the LDAP server (in the example, **uid=kgarrick,cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com**) and enter the **Password**.

|                    |   |
|--------------------|---|
| Distinguished Name | dc=fortinet,dc=com  |
|                    | <b>Fetch DN</b>   |
| Bind Type          | <input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular |
| User DN            | uid=kgarrick,cn=HeadOffice,ou=techdoc,dc=fortin   |
| Password           | .....   |

The **User DN** is an account that the FortiGate uses to query the LDAP server.

Select **Fetch DN** to determine a successful connection. If successful, a dropdown menu will appear showing the LDAP Tree, **dc=fortinet,dc=com**.

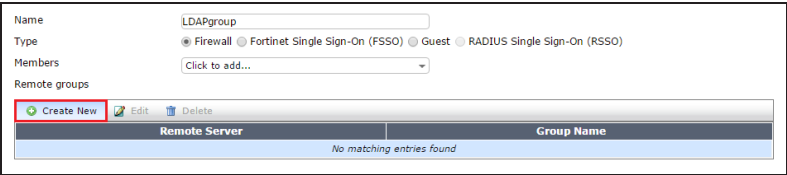
*If you select **Test**, it should show that the connection is **Successful**, however this is a false declaration. Only selecting **Fetch DN** will determine a successful connection.*



#### 4. Create the LDAP User Group on the FortiGate

Go to **User & Device > User > User Groups**, and select **Create New**.

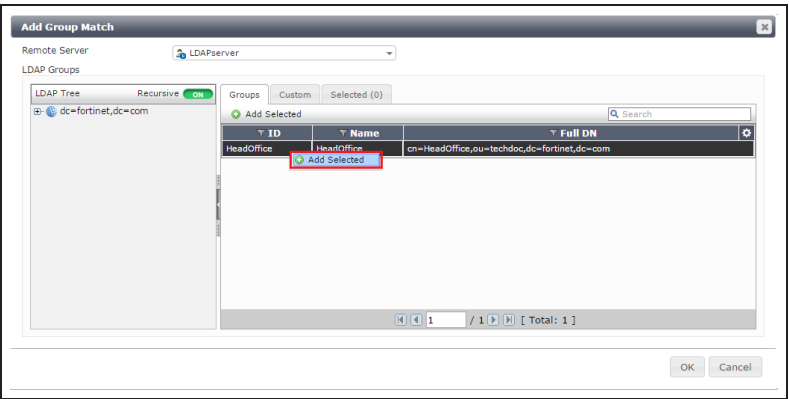
Enter a name for the user group, and under **Remote Groups**, select **Create New**.



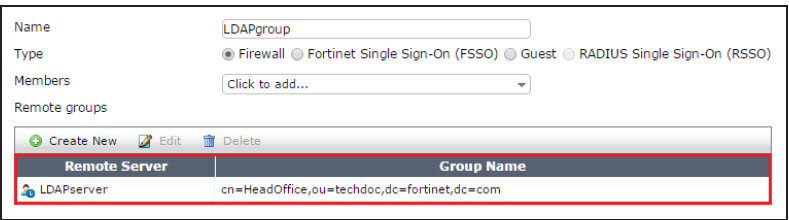
Select **LDAPserver** under the **Remote Server** dropdown.



In the new **Add Group Match** window, select **HeadOffice** under the **Groups** tab, and select **Add Selected**, then click **OK**.



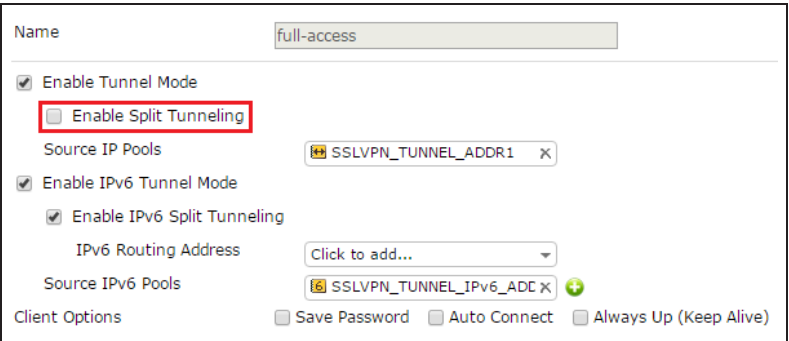
**LDAPserver** has been added to the LDAP group.



## 5. Configure the SSL VPN

From the FortiGate GUI, go to **VPN > SSL > Portals**, and edit the **full-access** portal.

Disable **Split Tunneling**.



Go to VPN > SSL > Settings.

Under **Connection Settings** set **Listen on Port** to 10443.

Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges** and set it to SSLVPN\_TUNNEL\_ADDR1.

Under **Authentication/Portal Mapping**, select **Create New**.

Connection Settings

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

wan1

This is generally your external interface (i.e. wan1)

Listen on Port

10443

Web mode access will be listening at https://172.20.121.56:10443, https://[2607:f0b0:f420:172:20:120:81]:10443

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout

Logout users when inactive for specified period

Never logout inactive users

Inactive For

300

(Seconds)

Server Certificate

Fortinet\_Factory

Default built-in certificate

Require Client Certificate

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range

Automatically assign addresses

Specify custom IP ranges

IP Ranges

SSLVPN\_TUNNEL\_ADDR1

DNS Server

Same as client system DNS

Specify

Specify WINS Servers

Allow Endpoint Registration

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Create New

Edit

Delete

| Users/Groups           | Realm | Portal     |
|------------------------|-------|------------|
| All Other Users/Groups | /     | web-access |

Assign the LDAPgroup user group to the full-access portal, and assign All Other Users/Groups to the desired portal.

Create New

Edit

Delete

| Users/Groups           | Realm | Portal      |
|------------------------|-------|-------------|
| LDAPgroup              | /     | full-access |
| All Other Users/Groups | /     | full-access |

Select the prompt at the top of the screen to create a new SSL-VPN policy.

Set **Source User(s)** to the LDAPgroup user group.

Set **Outgoing Interface** to wan1 and **Destination Address** to all.

Set **Service** to ALL and ensure that you enable NAT.

Incoming Interface

ssl.root (SSL VPN interface)

Source Address

all

Source User(s)

LDAPgroup

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

NAT

## 6. Results

From a remote device, access the SSL VPN Web Portal.

Enter valid LDAP credentials (in the example, *bwayne*).

Please Login

Name:

bwayne

Password:

••••••••

Login

'bwayne' is now successfully logged into the SSL VPN Portal.

Welcome to SSL VPN Service

Session Information

Time Logged In: bwayne (0 hour(s), 0 minute(s), 41 second(s))  
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes  
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Login History

| Time                   | Time Logged In | Inbound/Outbound Traffic |
|------------------------|----------------|--------------------------|
| 8/13/2015, 11:20:25 AM | 31 Seconds     | 0 B / 0 B                |

FortiClient Download

2

FortiClient Windows  

1

FortiClient Mac  

1

FortiClient iOS  

1

FortiClient Android

Tunnel Mode

The Fortinet SSL-VPN Client plugin is not installed on your computer, is not up to date, or your browser settings are blocking the plugin from running. The plugin is required for the tunnel mode function of the SSL-VPN Client.  
  
You need to have administrator rights to perform the first time installation. Once it is installed, it runs under normal user privileges and can be upgraded to newer versions without administrator privileges.

Connection Tool

Type: HTTP/HTTPS  
Host:  

Go

My Bookmarks

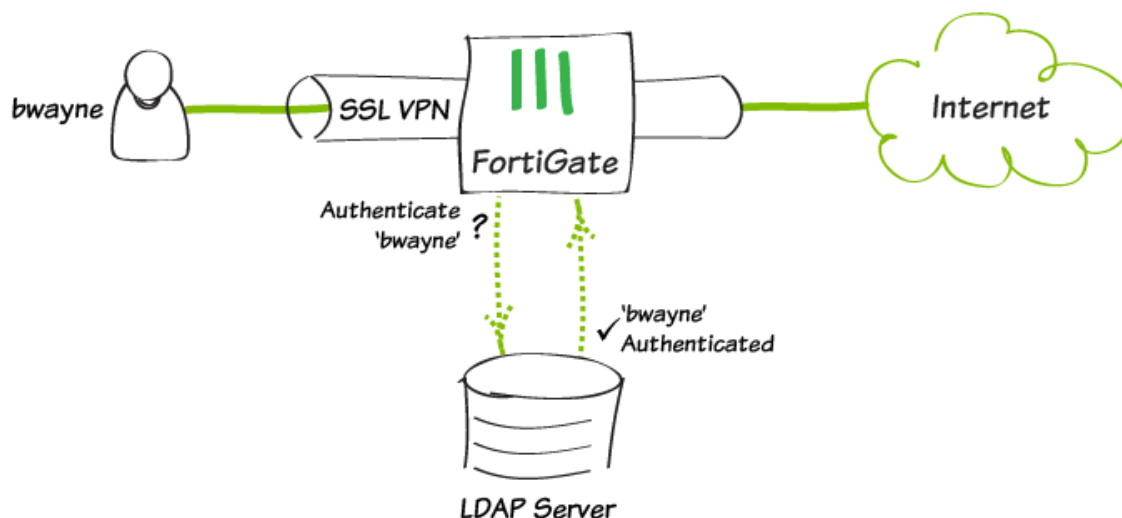
Add

Edit

From the FortiGate GUI, go to **VPN > SSL > Monitor** to confirm the connection.

|                                     | No. | User   | Source IP     | Begin Time               | Description |
|-------------------------------------|-----|--------|---------------|--------------------------|-------------|
| <input checked="" type="checkbox"/> | 1   | bwayne | 172.20.120.91 | Thu Aug 13 10:42:53 2015 |             |

# SSL VPN remote browsing with LDAP authentication



This recipe describes how to configure an SSL VPN tunnel using LDAP Authentication on a FortiAuthenticator.

The VPN will be tested using FortiClient on a mobile Android device.

The recipe assumes that an LDAP server has already been configured and connected on the FortiGate, containing the user 'bwayne'. For instructions on configuring FortiAuthenticator as an LDAP server, see [LDAP authentication for SSL VPN with FortiAuthenticator](#).

## 1. Creating the LDAP user group

From the FortiGate GUI, go to **User & Device > User > User Groups**, and select **Create New**.

Enter a name for the user group, and under **Remote Groups**, select **Create New**.



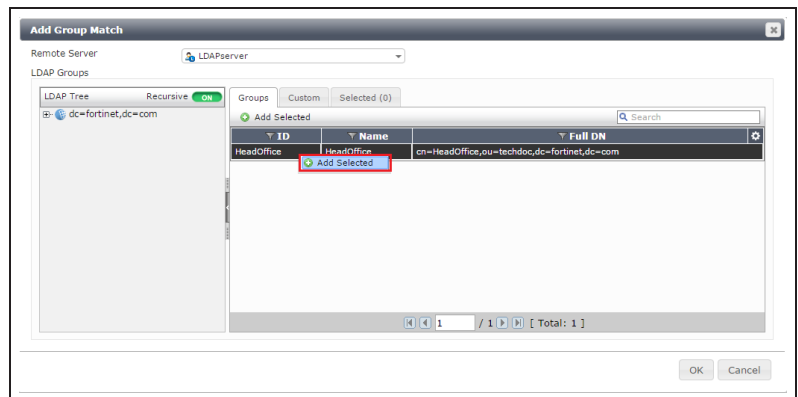
| Remote Server             | Group Name |
|---------------------------|------------|
| No matching entries found |            |

Select the LDAP server under the **Remote Server** dropdown.

*This part of the recipe assumes that an LDAP server has already been configured and connected on the FortiGate, containing the user 'bwayne'.*

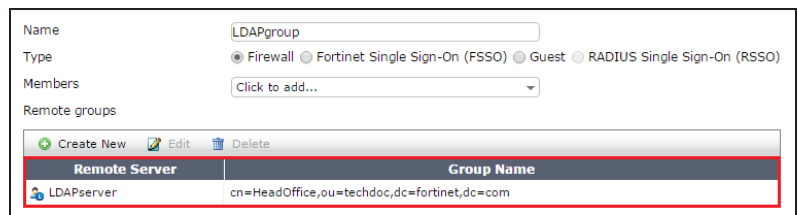


In the new **Add Group Match** window, select the desired group under the **Groups** tab, select **Add Selected**, and click **OK**.



| ID         | Name       | Full DN                                     |
|------------|------------|---|
| HeadOffice | HeadOffice | cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com |

The LDAP server has been added to the LDAP group.



| Remote Server | Group Name                                  |
|---------------|---|
| LDAPserver    | cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com |

## 2. Configuring the SSL VPN

Go to **VPN > SSL > Portals**, and edit the **full-access** portal.

Disable **Split Tunneling**.

Name

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools

☒ Enable IPv6 Tunnel Mode

☒ Enable IPv6 Split Tunneling

IPv6 Routing Address

Source IPv6 Pools

Client Options ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

Go to **VPN > SSL > Settings**.

Under **Connection Settings** set **Listen on Port** to **10443**.

Under **Authentication/Portal Mapping**, select **Create New**.

**Connection Settings**

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

Listen on Port

Restrict Access ☒ Allow access from any host ☐ Limit access to specific hosts

Idle Logout ☒ Logout users when inactive for specified period ☐ Never logout inactive users

Inactive For  (Seconds)

Server Certificate

Require Client Certificate ☐

**Tunnel Mode Client Settings**

Once connected in tunnel mode, clients will receive these settings.

Address Range ☐ Automatically assign addresses ☒ Specify custom IP ranges

IP Ranges

DNS Server ☒ Same as client system DNS ☐ Specify

Specify WINS Servers ☐

Allow Endpoint Registration ☐

**Authentication/Portal Mapping**

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

| Users/Groups           | Realm | Portal     |
|------------------------|-------|------------|
| All Other Users/Groups | /     | web-access |



Assign the **LDAPgroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal.

Edit Authentication/Portal Mapping

Users/Groups

LDAPgroup

Realm

/

Portal

full-access

OK

Cancel

### 3. Creating the security policies for VPN access to the Internet

Go to **Policy & Objects > Policy > IPv4** and create an **ssl.root - wan1** policy.

Set **Source User(s)** to the **LDAPgroup** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

Incoming Interface

ssl.root (SSL VPN interface)

Source Address

all

Source User(s)

LDAPgroup

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

 NAT

If it is not already available, create another policy allowing internal access to the Internet.

Incoming Interface

lan

Source Address

all

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

Firewall / Network Options

ON

 NAT

Use Outgoing Interface Address

Use Dynamic IP Pool

Use Central NAT Table

Fixed Port

Click to add...

## 4. Results

On your Android smartphone, open the FortiClient app and create a new VPN.

Give the VPN a name (in the example, *SSL to 121.56*), and set the **VPN Type** to **SSL VPN**. Select **Create**.



FortiClient VPN

Add VPN

VPN Name: SSL to 121.56

VPN Type:

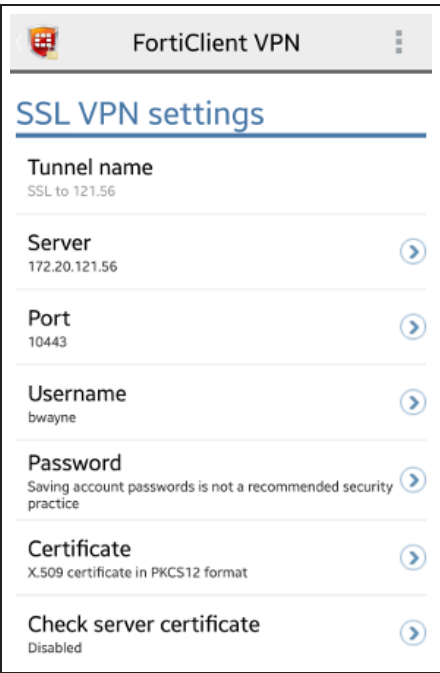
☒ SSL VPN

☐ IPsec VPN

Create

The SSL VPN settings will appear. Set **Server** to the IP of the FortiGate (in the example, *172.20.121.56*), and set the **Port** to *10443*.

Set **Username** to the desired LDAP user (in the example, *bwayne*), and set the user's password.



FortiClient VPN

SSL VPN settings

Tunnel name  
SSL to 121.56

Server  
172.20.121.56

Port  
10443

Username  
bwayne

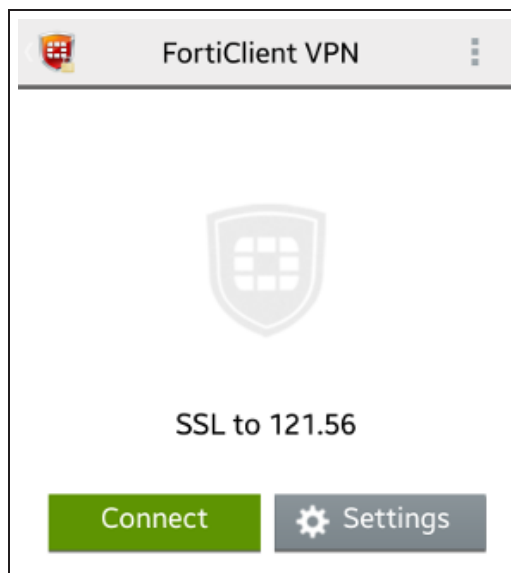
Password  
Saving account passwords is not a recommended security practice

Certificate  
X.509 certificate in PKCS12 format

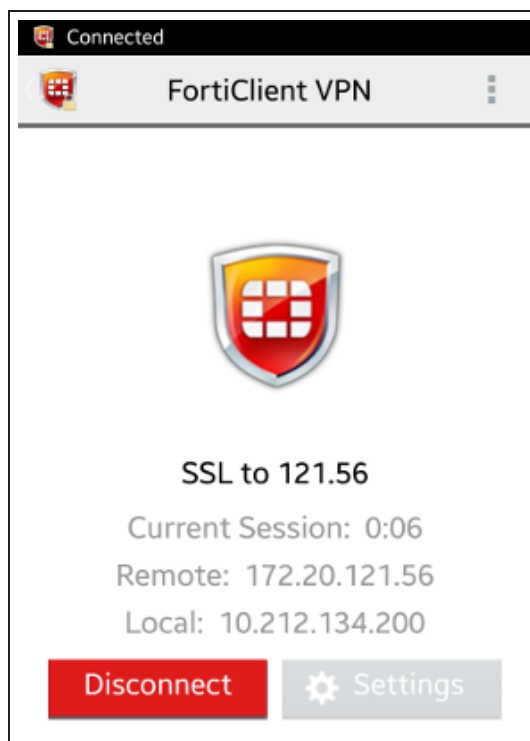
Check server certificate  
Disabled

Return to FortiClient's list of VPN Tunnels, and connect to the newly created SSL VPN.

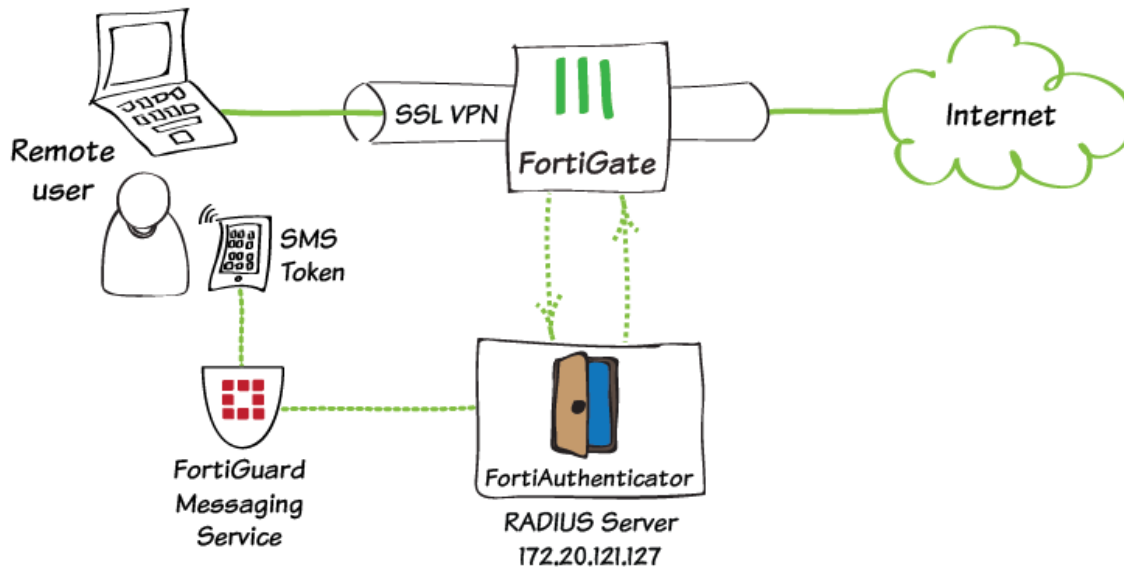
If prompted, enter valid LDAP credentials.



User 'bwayne' is now connected to the SSL VPN tunnel and can securely browse the Internet.



# SMS two-factor authentication for SSL VPN



In this recipe, you will create an SSL VPN with two-factor authentication consisting of a username/password and an SMS token. The SMS token is generated by FortiAuthenticator using the FortiGuard Messaging Service.

When a user attempts to connect to this SSL VPN, they are prompted to enter their username and password. After successfully entering their credentials, they receive an SMS message on their mobile phone containing a 6-digit number (called the FortiToken Code). They must also enter this number to get access to the internal network and the Internet.

Although this recipe uses the FortiGuard Messaging Service, it will also work with any compatible SMS service you configure as an SMS Gateway.

## 1. Creating an SMS user and user group on the FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > Local Users** and add/modify a user to include **SMS Token-based authentication** and a **Mobile number** using the preferred **SMS gateway** as shown.

The **Mobile number** must be in the format:  
**+[international\_number]**.

Enable **Allow RADIUS authentication**.

The screenshot shows the configuration page for a user named 'jgarrick'. The 'Token-based authentication' section is highlighted with a red box, showing 'Token-based authentication' checked, 'Deliver token code by:' set to 'SMS (+1-6131234567)', and 'Allow RADIUS authentication' checked. The 'User Role' section shows 'Role:' set to 'User'. The 'User Information' section shows 'Mobile number:' set to '+1-6131234567' and 'SMS gateway:' set to 'FortiGuard Messaging Service', both highlighted with a red box. Other fields include 'First name:', 'Last name:', 'Email address:', 'Phone number:', 'Street address:', 'City:', 'State/Province:', 'Country:', 'Language:', and 'Organization:'.

Go to **Authentication > User Management > User Groups** and add the above user to a new SMS user group (in the example, 'SMSgroup').

The screenshot shows the configuration page for a user group named 'SMSgroup'. The 'Type:' is set to 'Local'. The 'Users:' section shows a list of 'Available users' with a search filter and a list of 'Selected users' containing 'jgarrick'. There are buttons for 'Choose all visible' and 'Remove all'.

## 2. Configuring the FortiAuthenticator RADIUS client

Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Name: RADIUSclient

Client name/IP: 172.20.121.56

Secret: .....

Enable captive portal: ☐ Credentials portal (URL: /caplogin/) ☐ Social portal (URL: /social\_login/) ☐ MAC address portal (URL: /mlogin/)

Profiles

Profile name: Default

Description:

Apply this profile based on RADIUS attributes:

Authentication method: ☒ Enforce two-factor authentication ☐ Apply two-factor authentication if available (authenticate any user) ☐ Password-only authentication (exclude users without a password) ☐ FortToken-only authentication (exclude users without a FortToken)

Username input format: ☒ username@realm ☐ realmusername ☐ realmusername

Realms:

| Default                          | Realm               | Allow local users to override remote users | Use Windows AD domain authentication | Groups  | Delete                                |
|----------------------------------|---------------------|--|--------------------------------------|---|---------------------------------------|
| <input checked="" type="radio"/> | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | <input checked="" type="checkbox"/> Filter: SMSGroup (100%)<br>Users: (0/0) | <input type="button" value="Delete"/> |

Allow MAC-based authentication: ☐

Check machine authentication: ☐

EAP types: ☐ EAP-GTC ☐ EAP-TLS ☐ PEAP ☐ EAP-TTLS

Save

OK Cancel

Choose to **Enforce two-factor authentication** and add the SMS user group to the **Realms** group filter as shown.

Select **Save** and then **OK**.

## 3. Configuring the FortiGate authentication settings

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP address and pre-shared secret.

Use the **Test Connectivity** button to make sure that the FortiGate can communicate with the FortiAuthenticator.

Name: FAC-RADIUS

Primary Server IP/Name: 172.20.121.127

Primary Server Secret: .....

Secondary Server IP/Name:

Secondary Server Secret:

Authentication Method: ☒ Default ☐ Specify

NAS IP / Called Station ID:

Include in every User Group: ☐

Test Connectivity

Test Connectivity

Next, go to **User & Device > User > User Groups** and create a RADIUS user group called **RADIUSgroup**.

Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

NameRADIUSgroup

Type (RSSO)

☒ Firewall

☐ Fortinet Single Sign-On (FSSO)

☐ Guest

☐ RADIUS Single Sign-On

Members

Click to add...

Remote groups

Create NewEditDelete

| Remote Server | Group Name |
|---------------|------------|
| FAC-RADIUS    | Any        |

## 4. Configuring the SSL VPN

Go to **VPN > SSL > Settings**.

Under **Connection Settings**, set **Listen on Port** to **10443** and set **IP Ranges** to the SSL VPN tunnel address range.

Under **Authentication/Portal Mapping**, select **Create New**.

Assign the **RADIUSgroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal.

Connection Settings

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)wan1

This is generally your external interface (i.e. wan1)

Listen on Port10443

Web mode access will be listening at https://172.20.121.56:10443

Restrict Access

☒ Allow access from any host

☐ Limit access to specific hosts

Idle Logout

☒ Logout users when inactive for specified period

☐ Never logout inactive users

Inactive For300 (Seconds)

Server CertificateFortinet\_Factory

Require Client Certificate☐

Default built-in certificate

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range

☐ Automatically assign addresses

☒ Specify custom IP ranges

IP RangesSSLVPN\_TUNNEL\_ADDR1

DNS Server

☒ Same as client system DNS

☐ Specify

Specify WINS Servers☐

Allow Endpoint Registration☐

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Create NewEditDelete

| Users/Groups           | Realm | Portal      |
|------------------------|-------|-------------|
| RADIUSgroup            | /     | full-access |
| All Other Users/Groups | /     | full-access |

## 5. Creating the security policy for VPN access to the Internet

Go to **Policy & Objects > Policy > IPv4** and create an **ssl.root - wan1** policy.

Set **Source User(s)** to the **RADIUSgroup** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

|                                   |                              |
|-----------------------------------|------------------------------|
| Incoming Interface                | ssl.root (SSL VPN interface) |
| Source Address                    | all                          |
| Source User(s)                    | RADIUSgroup                  |
| Outgoing Interface                | wan1                         |
| Destination Address               | all                          |
| Schedule                          | always                       |
| Service                           | ALL                          |
| Action                            | ACCEPT                       |
| <b>Firewall / Network Options</b> |                              |
| ON NAT                            |                              |

## 6. Results

In this example, we will use the web portal to access the SSL VPN and test the two-factor authentication.

Open a browser and navigate to the SSL VPN web portal, in this case <https://172.20.121.56:10443>.

Enter a valid username and password and select **Login**. You should be prompted to enter a **FortiToken Code**.

### Please Login

**Name:** jgarrick

**Password:** .....

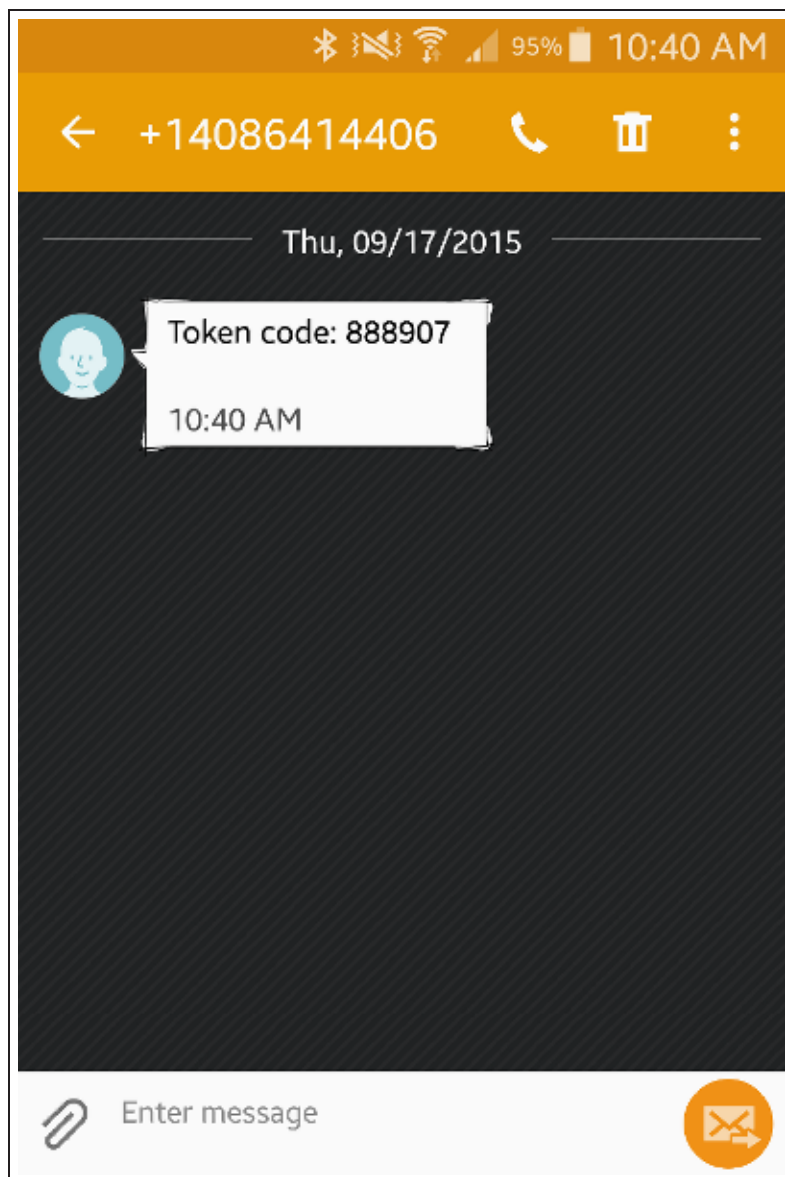
**FortiToken Code:**

Login



The **FortiToken Code** should have been sent to your mobile phone as a text message containing a 6-digit number.

Enter the number into the SSL VPN login portal and select **Login**.



You should now have access to the SSL VPN tunnel.

Welcome to SSL VPN Service

HelpLogout

Session Information

Time Logged In: jgarrick (0 hour(s), 0 minute(s), 0 second(s))  
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes  
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Login History

No login history found.

FortiClient Download

[FortiClient Windows](#)  
[FortiClient Mac](#)  
[FortiClient iOS](#)  
[FortiClient Android](#)

Tunnel Mode

The Fortinet SSL-VPN Client plugin is not installed on your computer, is not up to date, or your browser settings are blocking the plugin from running. The plugin is required for the tunnel mode function of the SSL-VPN Client.  
  
You need to have administrator rights to perform the first time installation. Once it is installed, it runs under normal user

Connection Tool

Type: HTTP/HTTPS  
Host:

My Bookmarks

To verify that the user has connected to the tunnel, go to **VPN > Monitor > SSL-VPN Monitor**.

| Delete                   |     |          |               |                          |             |
|--------------------------|-----|----------|---------------|--------------------------|-------------|
|                          | No. | User     | Source IP     | Begin Time               | Description |
| <input type="checkbox"/> | 1   | jgarrick | 172.20.120.56 | Tue Sep 22 11:56:50 2015 |             |

# SSL VPN troubleshooting

This page contains tips to help you with some common challenges for SSL VPN.

## There is no response from the SSL VPN URL.

Go to **VPN > SSL > Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.

## You receive an error stating that the web page cannot be found.

Check the URL you are attempting to connect to. It should follow this pattern:

*https://:remote/login.*

Ensure that you are using the correct port number for the part of the URL.

## FortiClient cannot connect.

Read the [Release Notes](#) to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

When you attempt to connect using FortiClient or in Web mode, you receive the following error message: “Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12).”

Ensure that cookies are enabled in your browser. Also, if you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.

## The tunnel connects but there is no communication.

Go to **Router > Static > Static Routes** (or **System > Network > Routing** on some FortiGate models) and ensure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Go to **Policy & Objects > Policy > IPv4** and check the policy allowing VPN access to the local network. If the destination address is set to all, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

**Users are unable to download the SSL VPN plugin.**

Go to **VPN > SSL > Portals** to check the VPN Portal to ensure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

**Users are being assigned to the wrong IP range.**

Ensure that the same IP Pool is used in VPN Portal and VPN Settings to avoid conflicts. If there is a conflict, the portal settings will be used.

# WiFi

These recipes describe how to use FortiAPs to add WiFi (or Wi-Fi) services to your network.

FortiAPs, managed by FortiGates, provide a full suite of WiFi features. Small offices can use FortiAPs to quickly add WiFi. Enterprises and educational institutions can take advantage of FortiAP access control features. Each WiFi network, or SSID, is represented by a WiFi network interface to which you can apply firewall policies, security profiles, and other features in the same way you would for wired networks.

## Getting started with WiFi

- [Setting up WiFi with FortiAP](#)
- [Setting up a WiFi bridge with a FortiAP](#)
- [Combining WiFi and wired networks with a software switch](#)
- [WiFi network with external DHCP service](#)
- [Providing remote access to the office and Internet](#)
- [Extending WiFi range with mesh topology](#)

## WiFi with other technologies

- [Explicit proxy with web caching](#)
- [AirPlay for Apple TV](#)

## WiFi local authentication

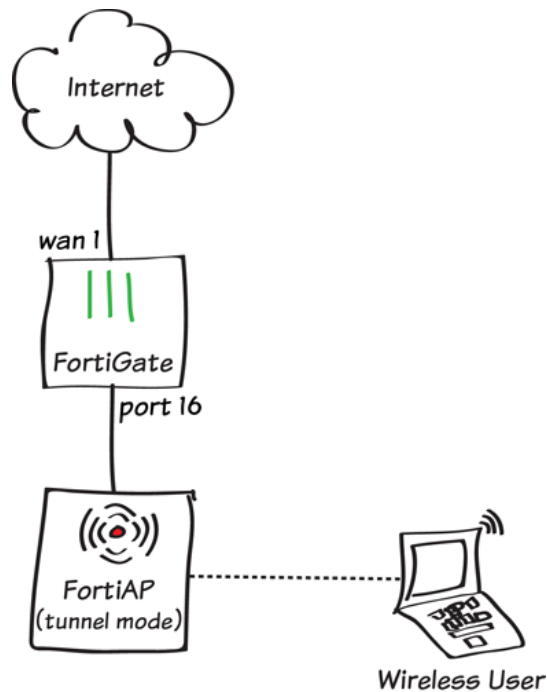
- [Guest WiFi accounts](#)
- [Captive portal WiFi access control](#)
- [WP2A WiFi access control](#)
- [MAC access control](#)
- [BYOD scheduling](#)
- [BYOD for a user with multiple wireless devices](#)

## WiFi remote authentication

- [WiFi RADIUS authentication with FortiAuthenticator](#)
- [Using an external captive portal for WiFi security](#)
- [Assigning WiFi users to VLANs dynamically](#)

- WiFi with Wireless Single Sign-on
- RSSO WiFi access control
- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)

# Setting up WiFi with FortiAP



In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Tunnel mode, allowing wireless access to the network.

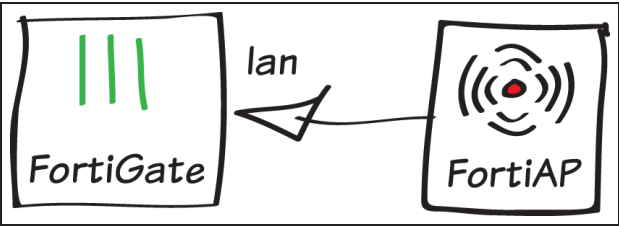
You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Bridge mode, see [Setting up a WiFi bridge with a FortiAP](#).

A video of this recipe is available [here](#).

# 1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the lan interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

| Mesh | Access Point     | State | Connected Via   |
|------|------------------|-------|-----------------|
| ▣    | FAP11C3X13000412 | ?     | 🖨️ 192.168.10.2 |

*The FortiAP may not appear until a few minutes have passed.*

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

| Mesh | Access Point     | State | Connected Via   |
|------|------------------|-------|-----------------|
| ▣    | FAP11C3X13000412 | ✓     | 🖨️ 192.168.10.2 |



## 2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**.

Select an **IP/Network Mask** for the wireless interface and enable **DHCP Server**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

| Interface Name        | <input type="text" value="wireless"/>  |             |        |             |              |
|-----------------------|--|-------------|--------|-------------|--------------|
| Type                  | <input type="text" value="WiFi SSID"/>   |             |        |             |              |
| Traffic Mode          | <input type="text" value="Tunnel to Wireless Controller"/>   |             |        |             |              |
| IP/Network Mask       | <input type="text" value="10.10.10.10/255.255.255.0"/>   |             |        |             |              |
| Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access |             |        |             |              |
| DHCP Server           | <input checked="" type="checkbox"/> Enable   |             |        |             |              |
| Address Range         | <div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.10.11</td><td>10.10.10.254</td></tr></tbody></table></div>  | Starting IP | End IP | 10.10.10.11 | 10.10.10.254 |
| Starting IP           | End IP   |             |        |             |              |
| 10.10.10.11           | 10.10.10.254   |             |        |             |              |
| Netmask               | <input type="text" value="255.255.255.0"/>   |             |        |             |              |
| Default Gateway       | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |             |              |
| DNS Server            | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify  |             |        |             |              |
|                       | <a href="#">Advanced...</a>  |             |        |             |              |
| WiFi Settings         |  |             |        |             |              |
| SSID                  | <input type="text" value="myWiFi"/>  |             |        |             |              |
| Security Mode         | <input type="text" value="WPA2 Personal"/>   |             |        |             |              |
| Pre-shared Key        | <input type="text" value="....."/> (8 - 63 characters)   |             |        |             |              |

### 3. Creating a custom FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

Name

myprofile

Comments

Write a comment...

0/255

Platform

FAP11C

▼ Radio 1

Mode

☐ Disable ☒ Access Point

Spectrum Analysis

☐

WIDS Profile

Click to set...

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4GHz 802.11n/g/b

Channel

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11


Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

 wireless (SSID: myWiFi) X

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.



Wireless Settings

FortiAP Profile

myprofile

Override Settings

Radio Settings Summary

| Radio   | Settings  | Channels | SSIDs   |
|---------|---|----------|---|
| Radio 1 |  AP (2.4 GHz Band) | 1, 6, 11 |  wireless (SSID: myWiFi) |

## 4. Allowing wireless access to the Internet

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the SSID and **Outgoing Interface** to your Internet-facing interface. Ensure that **NAT** is turned **ON**.

|  |                                     |   |
|--|-------------------------------------|---|
| Incoming Interface   | wireless (SSID: myWiFi)             | + |
| Source Address   | all                                 | + |
| Source User(s)   | Click to add...                     |   |
| Source Device Type   | Click to add...                     |   |
| Outgoing Interface   | wan1                                | + |
| Destination Address  | all                                 | + |
| Schedule   | always                              |   |
| Service  | ALL                                 | + |
| Action   | ACCEPT                              |   |
| <b>Firewall / Network Options</b>                                  |                                     |   |
| <input checked="" type="checkbox"/> NAT                            |                                     |   |
| <input checked="" type="radio"/> Use Destination Interface Address | <input type="checkbox"/> Fixed Port |   |
| <input type="radio"/> Use Dynamic IP Pool                          | Click to add...                     |   |

## 5. Results

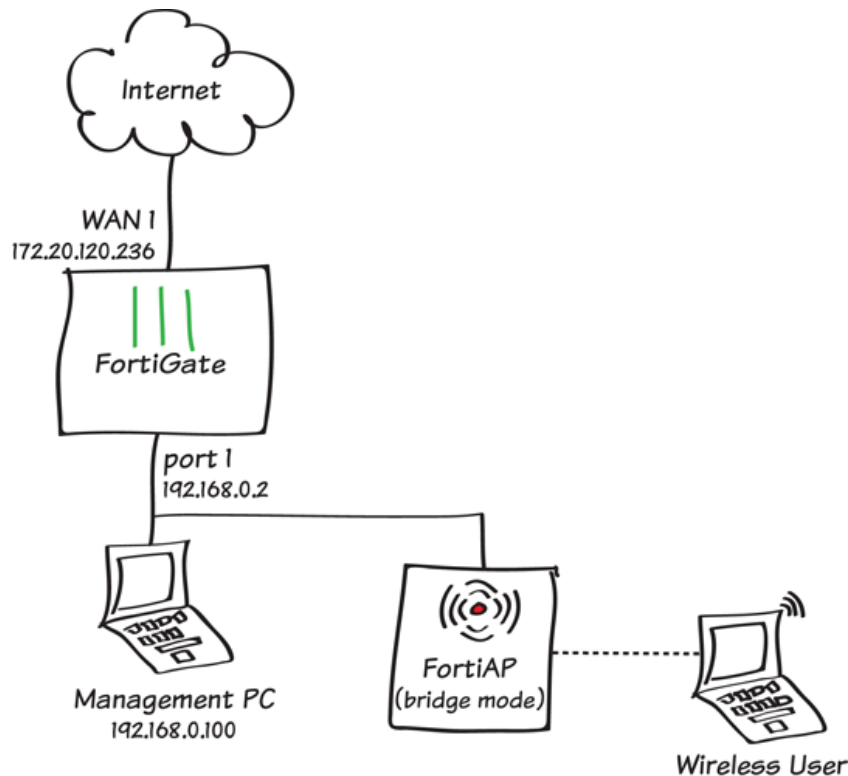
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.

| Mesh | Access Point     | State | Connected Via   |
|------|------------------|-------|-----------------|
| ■    | FAP11C3X13000412 | ✓     | 🖨️ 192.168.10.2 |

Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out [Configuring a WiFi LAN](#) in the [FortiOS 5.2 Handbook](#).

# Setting up a WiFi bridge with a FortiAP



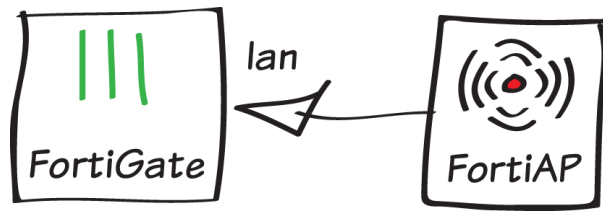
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Bridge mode.

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Tunnel mode, see [Setting up WiFi with FortiAP](#).

## 1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the **lan** interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

| Mesh | Access Point     | State | Connected Via |
|------|------------------|-------|---------------|
| ■    | FAP11C3X13000412 | ?     | 192.168.10.2  |

*The FortiAP may not appear until a few minutes have passed.*

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

| Mesh | Access Point     | State | Connected Via |
|------|------------------|-------|---------------|
| ■    | FAP11C3X13000412 | ✓     | 192.168.10.2  |

## 2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Local bridge with FortiAP's Interface**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

|   |                                       |
|---|---------------------------------------|
| Interface Name  | wireless                              |
| Type  | WiFi SSID                             |
| Traffic Mode  | Local bridge with FortiAP's Interf... |
| WiFi Settings   |                                       |
| SSID  | myWiFi                                |
| Security Mode   | WPA2 Personal                         |
| Pre-shared Key  | ..... (8 - 63 characters)             |
| Allow New WiFi Client Connections When Controller Is Down | <input type="checkbox"/>              |
| Maximum Clients   | <input type="checkbox"/>              |
| Optional VLAN ID  | 0                                     |

### 3. Creating a custom FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

Name

myprofile

Comments

Write a comment...

0/255

Platform

FAP11C

▼ Radio 1

Mode

☐ Disable

☒ Access Point

Spectrum Analysis

☐

WIDS Profile

Click to set...

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4GHz 802.11n/g/b

Channel

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

wireless (SSID: myWiFi) X

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.

Wireless Settings

FortiAP Profile

myprofile

☐ Override Settings

Radio Settings Summary

| Radio   | Settings          | Channels | SSIDs                   |
|---------|-------------------|----------|-------------------------|
| Radio 1 | AP (2.4 GHz Band) | 1, 6, 11 | wireless (SSID: myWiFi) |

## 4. Results

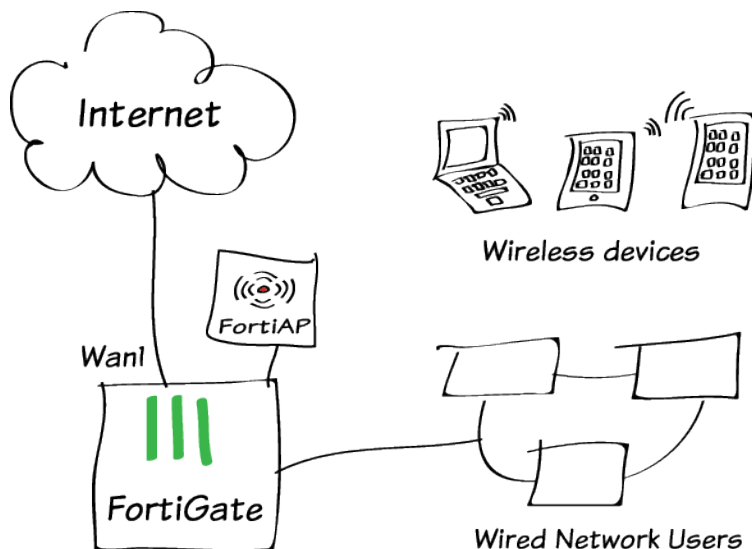
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.

| Mesh | Access Point     | State | Connected Via  |
|------|------------------|-------|--|
| ▣    | FAP11C3X13000412 | ✓     |  192.168.10.2 |

Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out [Bridge SSID to FortiGate wired network](#) in the [FortiOS 5.2 Handbook](#).

# Combining WiFi and wired networks with a software switch



Including mobile (WiFi) users on your office LAN can be more convenient than putting them on a separate wireless network. The Software Switch feature of your FortiGate is a simple way to do this.

Software Switches are only available if your FortiGate is in Interface mode. For more information, see [Choosing your FortiGate's switch mode](#).



# 1. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

Leave the IP address empty. This is allowed.

You can use any type of security/authentication. In this example, your users must be members of the *employees* group to access the network.

|                          |  |
|--------------------------|--|
| Interface Name           | example-wifi   |
| Type                     | WiFi SSID  |
| Traffic Mode             | Tunnel to Wireless Controller  |
| IP/Network Mask          | <input type="text"/>   |
| WiFi Settings            |  |
| SSID                     | <input type="text" value="example-staff"/>                                 |
| Security Mode            | WPA2 Enterprise  |
| Authentication           | <input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server |
|                          | <input type="text" value="employees"/>                                     |
| Broadcast SSID           | <input checked="" type="checkbox"/>  |
| Block Intra-SSID Traffic | <input type="checkbox"/>   |
| Maximum Clients          | <input type="checkbox"/>   |
| Optional VLAN ID         | <input type="text" value="0"/>   |

# 2. Combine the WiFi and wired interfaces

Go to **System > Network > Interface**. Edit the existing **lan** software switch interface or create a new one.

Make sure your wired and WiFi interfaces are both included.

Make sure there is a **DHCP Server** configured. It will provide IP addresses to both WiFi and wired users.

| Interface Name             | lan  |             |        |              |                |
|----------------------------|--|-------------|--------|--------------|----------------|
| Type                       | Software Switch  |             |        |              |                |
| Physical Interface Members | <div><div>port1</div><div>example-wifi (SSID: exa...</div></div>   |             |        |              |                |
| Addressing mode            | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE   |             |        |              |                |
| IP/Network Mask            | <input type="text" value="192.168.65.1/255.255.255.0"/>  |             |        |              |                |
| Administrative Access      | <div><div><input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP</div><div><input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access</div></div> |             |        |              |                |
| DHCP Server                | <input checked="" type="checkbox"/> Enable   |             |        |              |                |
| Address Range              | <div><div>Create New Edit Delete</div><table><tr><th>Starting IP</th><th>End IP</th></tr><tr><td>192.168.65.2</td><td>192.168.65.254</td></tr></table></div>   | Starting IP | End IP | 192.168.65.2 | 192.168.65.254 |
| Starting IP                | End IP   |             |        |              |                |
| 192.168.65.2               | 192.168.65.254   |             |        |              |                |
| Netmask                    | <input type="text" value="255.255.255.0"/>   |             |        |              |                |
| Default Gateway            | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |              |                |
| DNS Server                 | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify   |             |        |              |                |

### 3. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing all users on the software switch interface to connect to the Internet.

Incoming Interface

lan

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1

+

Destination Address

all

+

Schedule

always

Service

ALL

+

Action

✓ ACCEPT

Firewall / Network Options

ON

NAT

☒ Use Outgoing Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

### 4. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**. Configure a network interface that is dedicated to extension devices.

Addressing mode

☐ Manual ☐ DHCP ☐ PPPoE ☒ Dedicated to Extension Device

IP/Network Mask

10.11.12.1/255.255.255.0

Connected Devices

None

Connect the FortiAP unit and wait for it to be listed in **WiFi Controller > Managed Access Points > Managed FortiAPs**.

| Create New Edit Delete Refresh |  |                  |       |               |                      |                        |                          |            |                 |
|--------------------------------|--|------------------|-------|---------------|----------------------|------------------------|--------------------------|------------|-----------------|
| Mesh                           |  | Access Point     | State | Connected Via | SSIDs                | Channel                | Clients                  | OS Version | FortiAP Profile |
| a                              |  | FP221C3X14019926 |       | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |            | FAP221C-default |

Highlight the FortiAP unit on the list and select **Authorize**.

# 5. Add the SSID to the FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model.

For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.

▼ Radio 2

Mode

☐ Disable ☒ Access Point

Spectrum Analysis

☐

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

5GHz 802.11ac/n/a ▼

Select Channel Width

20MHz ▼

Channel

☒ 36 ☐ 40 ☒ 44 ☐ 48 ☒ 149 ☐ 153 ☒ 157 ☐ 161 ☒ 165

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

example-wifi (SSID: exa... X

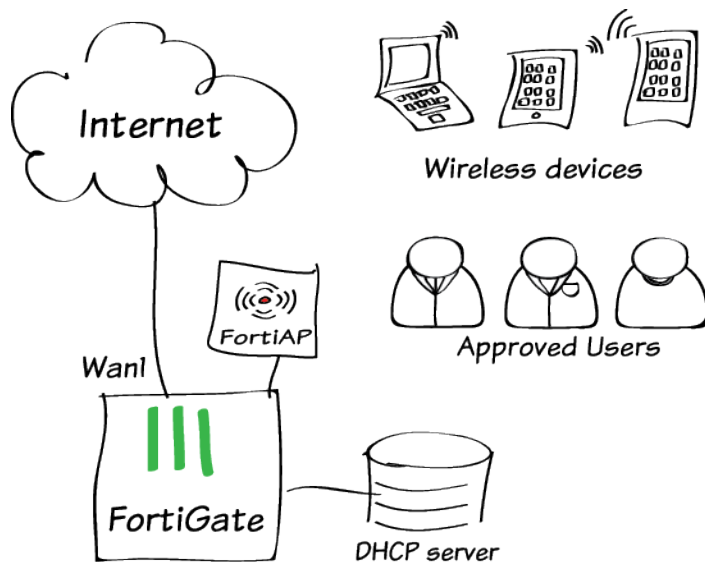
## Results

Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

| ▼ SSID        | ▼ FortiAP            | ▼ User | ▼ IP         | ▼ Device           | ▼ Channel | ▼ Bandwidth Tx/Rx   | ▼ Signal Strength |
|---------------|----------------------|--------|--------------|--------------------|-----------|---------------------|-------------------|
| example-staff | FP221C3X14019926 (1) | rgreen | 192.168.65.2 | 08:fd:0e:fff:0c:56 | 1         | 906 bps <div></div> | 30 dB             |

For further reading, check out **Software switch** in the **FortiOS 5.2 Handbook**.

# WiFi network with external DHCP service



In this example, you use an external DHCP server to assign IP addresses to your WiFi clients.

The DHCP server assigns IP addresses in the range of 10.10.12.100 to 10.10.12.200. The server is attached to Port 13 of the FortiGate and has an IP address of 10.10.13.254.

# 1. Configure the FortiGate network interface for the DHCP server

Go to **System > Network > Interfaces** and edit Port13.

The external DHCP server is on the 10.10.13.0 network, so put the interface on that network.

|                 |  |
|-----------------|--|
| Interface Name  | port13(08:5B:0E:1A:8A:FF)  |
| Alias           |  |
| Link Status     | Up   |
| Type            | Physical Interface   |
| Addressing mode | <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device |
| IP/Network Mask | 10.10.13.1/255.255.255.0   |

# 2. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

The DHCP server assigns IP addresses on the 10.10.12.0 network, so configure the SSID address on this network.

|                     |                               |
|---------------------|-------------------------------|
| Interface Name      | example-wifi                  |
| Type                | WiFi SSID                     |
| Traffic Mode        | Tunnel to Wireless Controller |
| IP/Network Mask     | 10.10.12.1/255.255.255.0      |
| IPv6 Address/Prefix | ::/0                          |

Enable **DHCP Server**, then expand **Advanced** and change the mode to **Relay**. Enter the external **DHCP server IP** address.

|                |  |
|----------------|--|
| DHCP Server    | <input checked="" type="checkbox"/> Enable                           |
| ▼ Advanced...  |  |
| Mode           | <input type="radio"/> Server <input checked="" type="radio"/> Relay  |
| DHCP Server IP | 10.10.13.254   |
| Type           | <input checked="" type="radio"/> Regular <input type="radio"/> IPsec |

Set up security and authentication for your SSID.

In this case, WPA2 Enterprise authentication allows access only to members of the *employees* user group.

|                          |  |
|--------------------------|--|
| WiFi Settings            |  |
| SSID                     | example-staff  |
| Security Mode            | WPA2 Enterprise  |
| Authentication           | <input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server |
|                          | employees  |
| Broadcast SSID           | <input checked="" type="checkbox"/>  |
| Block Intra-SSID Traffic | <input checked="" type="checkbox"/>  |
| Maximum Clients          | <input type="checkbox"/>   |
| Optional VLAN ID         | 0  |

### 3. Create the security policies

Create a policy to allow the WiFi network to communicate with the DHCP Server on Port 13.

The source and destination networks are directly visible to each other, so NAT is not required.

|                     |                                    |   |
|---------------------|------------------------------------|---|
| Incoming Interface  | example-wifi (SSID: example-staff) | + |
| Source Address      | all                                | + |
| Source User(s)      | Click to add...                    |   |
| Source Device Type  | Click to add...                    |   |
| Outgoing Interface  | port13                             | + |
| Destination Address | all                                | + |
| Schedule            | always                             |   |
| Service             | DHCP                               | + |
| Action              | ACCEPT                             |   |

**Firewall / Network Options**

☐ OFF ☐ NAT

Create a policy to allow WiFi clients to connect to the Internet on wan1.

|                     |                                    |   |
|---------------------|------------------------------------|---|
| Incoming Interface  | example-wifi (SSID: example-staff) | + |
| Source Address      | all                                | + |
| Source User(s)      | Click to add...                    |   |
| Source Device Type  | Click to add...                    |   |
| Outgoing Interface  | wan1                               | + |
| Destination Address | all                                | + |
| Schedule            | always                             |   |
| Service             | ALL                                | + |
| Action              | ACCEPT                             |   |

**Firewall / Network Options**

☒ ON ☐ NAT

### 4. Connect and authorize the FortiAP unit

Configure the network interface where the FortiAP will be connected.

|                   |  |
|-------------------|--|
| Addressing mode   | <input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicated to Extension Device |
| IP/Network Mask   | 10.11.12.1/255.255.255.0   |
| Connected Devices | None   |

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

*The FortiAP may not appear until a few minutes have passed.*

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile, adding your SSID to each radio.

Create NewEditDeleteRefresh

Display ByAPRadioManaged FortiAPs1/64

| Mesh | Access Point     | State | Connected Via | SSIDs                | Channel                | Clients                  | OS Version | FortiAP Profile |
|------|------------------|-------|---------------|----------------------|------------------------|--------------------------|------------|-----------------|
| ■    | FP221C3X14019926 | ?     | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |            | FAP221C-default |

Radio 2

Mode

☐ Disable☒ Access Point

Spectrum Analysis

☐

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff☐ AP Handoff

Band

5GHz 802.11ac/n/a

Select Channel Width

20MHz

Channel

☒ 36☐ 40☒ 44☐ 48☒ 149☐ 153☒ 157☐ 161☒ 165

Auto TX Power Control

☒ Disable☐ Enable

TX Power

100 %

SSID

X

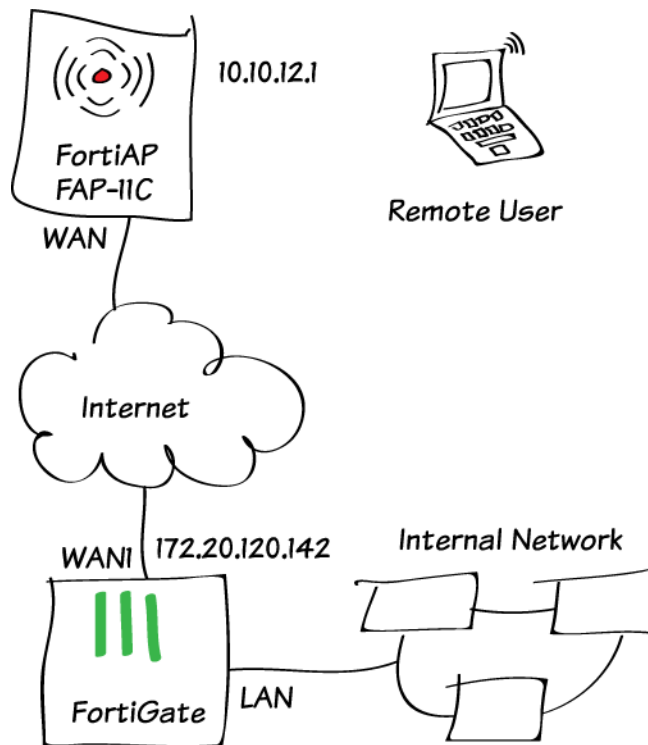
## Results

WiFi devices can connect to the Internet. You can see them in the client monitor (**WiFi Controller > Monitor > Client Monitor**). Note the IP addresses assigned by the external DHCP server.

| SSID          | FortiAP              | User  | IP           | Device            | Channel | Bandwidth Tx/Rx | Signal |
|---------------|----------------------|-------|--------------|-------------------|---------|-----------------|--------|
| example-staff | FP221C3X14019926 (2) | green | 10.10.12.100 | 08:fd:0e:ff:0c:56 | 165     | 6.52 Mbps       | 50     |

For further reading, check out the **Deploying Wireless Networks** in the **FortiOS 5.2 Handbook**.

# Providing remote access to the office and Internet



In this example, you pre-configure a FortiAP to provide access to the office network from any remote location simply by connecting the FortiAP to the Internet. This FortiAP could be given to an employee to use at home or when traveling.

The FortiAP's configuration also supports Internet browsing from behind the corporate firewall. The remote user's local network remains accessible by defining it as a split tunnel destination that is not routed through the FortiGate unit.



# 1. Enable the split tunneling feature

By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the CLI.

Go to **System > Dashboard > Status** and use the CLI Console.

```
config system global
set gui-fortiap-split-tunneling enable
end
```

# 2. Create the WiFi network

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID. The SSID will accept logons from the *employees* user group.

WiFi Settings

SSID

example-staff

Security Mode

WPA2 Enterprise

Authentication

☒ Local

☐ RADIUS Server

employees

+

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Split Tunneling

☒

Optional VLAN ID

0

Enable the DHCP Server and make note of the IP range.

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.10.12.2  | 10.10.12.254 |

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP

☐ Specify

DNS Server

☒ Same as System DNS

☐ Same as Interface IP

☐ Specify

▶ Advanced...

### 3. Create the security policy

Go to **Policy & Objects > Objects > Addresses** and create an address representing the range of remote user addresses that the DHCP server can assign.

|                   |                                     |
|-------------------|-------------------------------------|
| Name              | remote_users                        |
| Type              | IP Range                            |
| Subnet / IP Range | 10.10.12.2-10.10.12.254             |
| Interface         | example-wifi (SSID: example-staff)  |
| Visibility        | <input checked="" type="checkbox"/> |
| Comments          | <input type="text"/> 0/255          |

Go to **Policy & Objects > Policy > IPv4** and create a policy that allows remote wireless users to access the Internet and the corporate network.

|  |                                    |     |
|--|------------------------------------|-----|
| Incoming Interface   | example-wifi (SSID: example-staff) | +   |
| Source Address   | remote_users                       | +   |
| Source User(s)   | Click to add...                    |     |
| Source Device Type   | Click to add...                    |     |
| Outgoing Interface   | wan1                               | X + |
|  | lan                                | X   |
| Destination Address  | all                                | +   |
| Schedule   | always                             |     |
| Service  | ALL                                | +   |
| Action   | ACCEPT                             |     |
| <b>Firewall / Network Options</b>  |                                    |     |
| <input checked="" type="checkbox"/> NAT  |                                    |     |
| <input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Fixed Port |                                    |     |

## 4. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile for the FortiAP model you are using.

The **Split Tunneling Subnet(s)** entry exempts a typical home network subnet from being routed through the FortiGate.

Select the **SSID** that the remote FortiAP will broadcast.

The screenshot shows the configuration page for a FortiAP profile named 'FAP11C-remote'. The 'Name' field is 'FAP11C-remote', 'Comments' is empty, 'Platform' is 'FAP11C', and 'Split Tunneling Subnets(s)' is '192.168.1.0/24'. Under the 'Radio 1' section, 'Mode' is set to 'Access Point', 'WIDS Profile' is 'default', 'Radio Resource Provision' is checked, 'Client Load Balancing' is unchecked, 'Frequency Handoff' and 'AP Handoff' are unchecked, 'Band' is '2.4GHz 802.11n/g/b', 'Channel' is '1', 'Auto TX Power Control' is 'Disable', and 'TX Power' is a bar chart showing a gradient from low to high, with a slider at 100%. The 'SSID' field shows 'example-wifi (SSID: exa...' with a green plus icon. Under the 'LAN Port' section, 'Mode' is set to 'Bridge to' with a dropdown menu showing 'WAN Port'.

## 5. Enable CAPWAP on the Internet interface

Go to **System > Network > Interfaces** and edit the Internet-facing interface. In **Administrative Access**, enable CAPWAP.

The screenshot shows the 'Administrative Access' settings for an interface. The settings are: HTTPS (checked), PING (checked), HTTP (unchecked), FMG-Access (checked), CAPWAP (checked), SSH (checked), SNMP (unchecked), and FCT-Access (unchecked).

## 6. Pre-authorize the FortiAP unit

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.

Enter your FortiAP's **Serial Number** and a **Name** to identify whose device it is.

Choose the **FortiAP Profile** that you created.

The screenshot shows the configuration page for a Managed FortiAP. The 'Serial Number' is 'FAP11C3X13000412', 'Name' is 'rgreen-ap', 'Comments' is empty, 'State' is 'Authorized', and 'Wireless Settings' section shows 'FortiAP Profile' as 'FAP11C-remote' with an 'Override Settings' checkbox.

## 7. Configure the FortiAP unit

Use FortiExplorer to access the FortiAP CLI through the USB MGMT port.

Enter these commands to specify the IP address of the FortiGate WiFi controller, which will be the Internet-facing interface IP address. Enter *exit* to end.

```
FAP11C3X13000412 # login: admin
FAP11C3X13000412 # cfg -a AC_IPADDR_1=172.20.120.142
FAP11C3X13000412 # cfg -c
FAP11C3X13000412 # exit
```

The remote user can now take this device to a remote location to connect securely to the corporate FortiGate unit.

## Results

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power. The network must provide DHCP service and allow the FortiAP to access the internet.



Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller. The remote WiFi user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

Connections to destinations on the "split tunneling" network are possible, but will not be visible in the FortiGate logs as the traffic remains local to the FortiAP.

Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

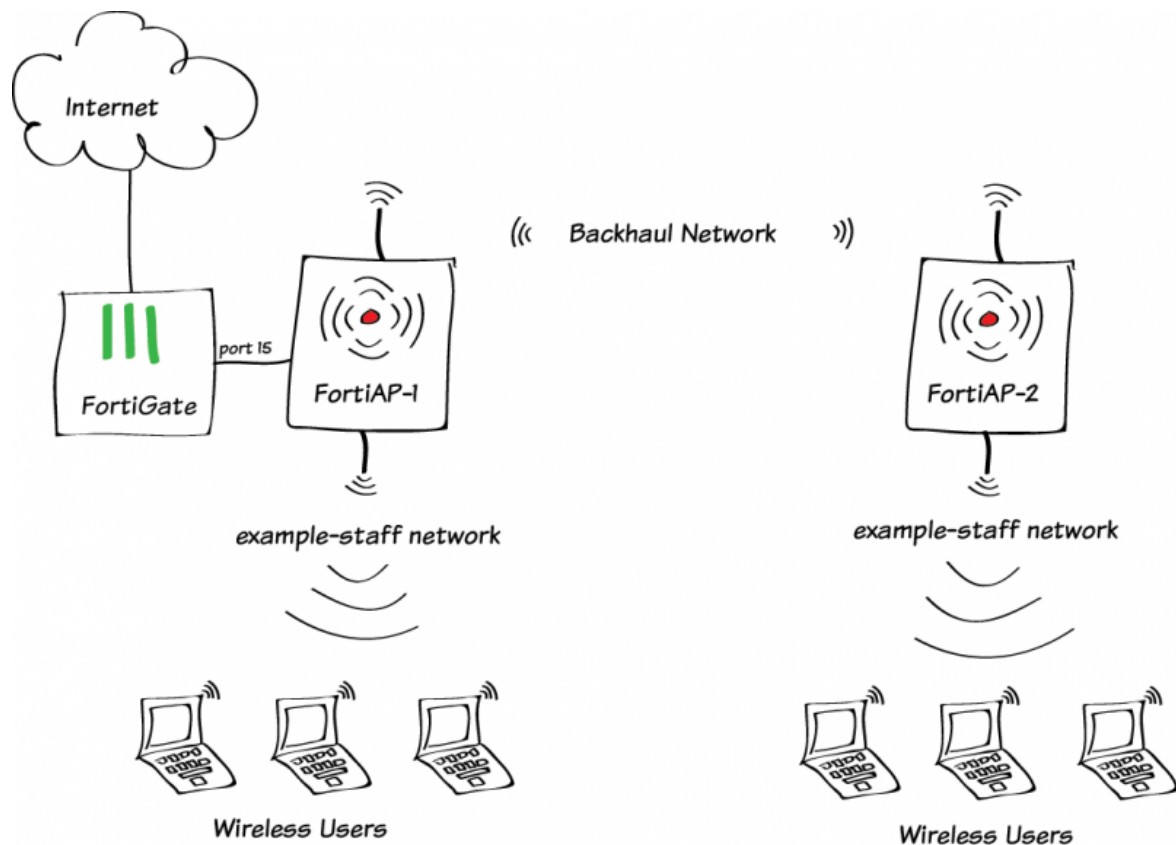
| SSID          | FortiAP       | User   | IP         | Device            | Channel | Bandwidth Tx/Rx | Signal Strength/Noise | Signal      |
|---------------|---------------|--------|------------|-------------------|---------|-----------------|-----------------------|-------------|
| example-staff | rgreen-ap (1) | rgreen | 10.10.12.4 | 08:fd:0e:ff:0c:56 | 6       | 328.97 Kbps     | 44 dB                 | <div></div> |

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs. Select an entry to view more information about remote traffic to the corporate network and to the Internet.

|               |   |                 |                          |
|---------------|---|-----------------|--------------------------|
| #             | 1   | Action          | ip-conn                  |
| Date/Time     | 11:46:46  | Destination     | 208.91.112.52            |
| Dst Interface | wan1  | Dst Port        | 53                       |
| Group         | employees   | Level           | INFO                     |
| Log ID        | 11  | Policy ID       | 8                        |
| Policy UUID   | 450ac232-ce5c-51e4-c482-a35b6764918e  | Sequence Number | 4011                     |
| Source        |  rgreen (10.10.12.4) | Source SSID     | example-staff            |
| Src Interface | example-wifi  | Src Name        | android-1b1c4f3382fb54b0 |
| Src Port      | 35023   | Sub Type        | forward                  |
| Threat        | 262144  | Threat Level    | medium                   |
| Threat Score  | 10  | Timestamp       | 4/30/2015, 11:46:46 AM   |
| User          |  rgreen              | Virtual Domain  | root                     |

For further reading, check out **Deploying Wireless Networks** in the **FortiOS 5.2 Handbook**.

# Extending WiFi range with mesh topology



In this example, two FortiAPs are used to extend the range of a single WiFi network. The second FortiAP is connected to the FortiGate WiFi controller through a dedicated WiFi backhaul network.

In this example, both FortiAPs provide the example-staff network to clients that are in range.

More mesh-connected FortiAPs could be added to further expand the coverage range of the network. Each AP must be within range of at least one other FortiAP. Mesh operation requires FortiAP models with two radios, such as the FortiAP-221C units used here.

# 1. Create the backhaul SSID

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID. Set **Traffic Mode** to **Mesh Downlink**.

You will need the pre-shared key when configuring the mesh-connected FortiAP.

|                |               |
|----------------|---------------|
| Interface Name | Backhaul_mesh |
| Type           | WiFi SSID     |
| Traffic Mode   | Mesh Downlink |

---

WiFi Settings

SSID

backhaul-ssid

Security Mode

WPA2 Personal

Pre-shared Key

.....

(8 - 63 characters)

---

Comments

0/255

Administrative Status

☒ Up ☐ Down

# 2. Create the client SSID

Go to **WiFi Controller > WiFi Network > SSID**. Create the WiFi network (SSID) that clients will use.

WiFi Settings

SSID

example-staff

Security Mode

WPA2 Enterprise

Authentication

☒ Local ☐ RADIUS Server

employees

+

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Optional VLAN ID

0

Configure DHCP for your clients.

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.10.12.2  | 10.10.12.254 |

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

Advanced...

### 3. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a profile for the Platform (FortiAP model) that you are using.

Configure Radio 1 for the client channel on the 2.4GHz 802.11n/g Band.

Configure Radio 2 for the backhaul channel on the 5GHz 802.11ac/n Band.

▼ Radio 1

Mode

☐ Disable ☒ Access Point ☐ Dedicated Monitor

Spectrum Analysis

☐

WIDS Profile

Click to set...

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4GHz 802.11n/g

Channel

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

example-wifi (SSID: exa... X

+

▼ Radio 2

Mode

☐ Disable ☒ Access Point

Spectrum Analysis

☐

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

5GHz 802.11ac/n

Select Channel Width

20MHz

Channel

☒ 36 ☐ 40 ☒ 44 ☐ 48 ☒ 149 ☐ 153 ☒ 157 ☐ 161 ☒ 165

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

Backhaul\_mesh (SSID: b... X

+

### 4. Configure the security policy

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Incoming Interface

example-wifi (SSID: example-staff) +

Source Address

all +

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

wan1 +

Destination Address

all +

Schedule

always +

Service

ALL +

Action

✓ ACCEPT

Firewall / Network Options

ON

NAT



## 5. Configure an interface dedicated to FortiAP

Go to **System > Network > Interfaces** and edit an available interface (in this example, port 15). Set **Addressing mode** to **Dedicate to Extension Device**.

|                   |  |
|-------------------|--|
| Addressing mode   | <input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicated to Extension Device |
| IP/Network Mask   | <input type="text" value="192.168.1.1/255.255.255.0"/>   |
| Connected Devices | 1 FortiAP(s)   |

## 6. Preauthorize FortiAP-1

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.

Enter the serial number of the FortiAP unit and give it a name. Select the FortiAP profile that you created earlier.

|                          |  |
|--------------------------|--|
| Serial Number            | <input type="text" value="FP221C3X14019926"/>  |
| Name                     | <input type="text" value="FortiAP-1"/>   |
| Comments                 | <input type="text" value=""/> 0/35   |
| State                    | Authorized   |
| <b>Wireless Settings</b> |  |
| FortiAP Profile          | <input type="text" value="FAP221C-mesh"/> <input type="checkbox"/> Override Settings |

## 7. Configure FortiAP-2 for mesh operation

Connect FortiAP-2 to Port 15.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. FortiAP-2, identified by serial number, will be listed within two minutes. Note the **Connected Via** IP address.

| Mesh                     | Access Point     | State | Connected Via | SSIDs  |
|--------------------------|------------------|-------|---------------|--|
| <input type="checkbox"/> | FP221C3X14023979 | ?     | 192.168.1.4   | Radio 1:<br>Radio 2:                             |
| <input type="checkbox"/> | FortiAP-1        | ✓     | -             | Radio 1: example-staff<br>Radio 2: backhaul-ssid |

Go to **System > Dashboard > Status**.

In the CLI Console, enter `exec telnet 192.168.1.4` (your address might be different) to log in to the FortiAP as *admin*. Enter the commands to change the AP to mesh uplink on the *backhaul-ssid* network. Enter *exit* to end.

Disconnect FortiAP-2 from the FortiGate. Install it in its planned location and apply power.

Connect FortiAP-1 to Port 15 and apply power.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. Select the FortiAP-2 entry (identified by serial number) and edit the new entry. Enter the **Name**, FortiAP-2. Select the **FortiAP Profile** that you created earlier. Click **Authorize**. Click **OK**.

```
FP221C3X14019926 login: admin
FP221C3X14019926 # cfg -a MESH_AP_TYPE=1
FP221C3X14019926 # cfg -a MESH_AP_SSID=backhaul-ssid
FP221C3X14019926 # cfg -a MESH_AP_PASSWD=backhaul-ssid-passwd
FP221C3X14019926 # cfg -c
FP221C3X14019926 # exit
```

Serial Number

FP221C3X14023979

Name

FortiAP-2

Comments

0/35

Managed AP Status

Status

Connecting

Connected Via

Mesh (192.168.1.2)

State

Discovered

Authorize

Wireless Settings

FortiAP Profile

FAP221C-mesh

Override Settings

Radio Settings Summary

| Radio   | Settings          | Channels | SSIDs                               |
|---------|-------------------|----------|-------------------------------------|
| Radio 1 | AP (2.4 GHz Band) | 11       | example-wifi (SSID: example-staff)  |
| Radio 2 | AP (5 GHz Band)   | 153      | Backhaul_mesh (SSID: backhaul-ssid) |

## 8. Connect and authorize the FortiAPs

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. The FortiAPs will be listed as online within about two minutes. (Click **Refresh** to update the display.)

| Mesh | Access Point | State | Connected Via | SSIDs  | Channel                   | Clients                  | OS Version     | FortiAP Profile |
|------|--------------|-------|---------------|--|---------------------------|--------------------------|----------------|-----------------|
|      | FortiAP-1    | ✓     | 192.168.1.3   | Radio 1: example-staff<br>Radio 2: backhaul-ssid | Radio1: 11<br>Radio2: 153 | Radio 1: 0<br>Radio 2: 1 | v5.2-build0237 | FAP221C-mesh    |
|      | FortiAP-2    | ✓     | 192.168.1.2   | Radio 1: example-staff<br>Radio 2: backhaul-ssid | Radio1: 0<br>Radio2: 0    | Radio 1: 0<br>Radio 2: 0 | v5.2-build0237 | FAP221C-mesh    |

# 9. Results

Go to **WiFi Controller > Monitor > Client Monitor**. Click **Refresh** to see updated information.

Use a mobile device near FortiAP-2 to connect to the *example-staff* network. The monitor shows the mobile user *rgreen* as a client of FortiAP-2.

Disconnect from the *example-staff* network and then reconnect near FortiAP-1. The monitor shows the mobile user *rgreen* as a client of FortiAP-1.

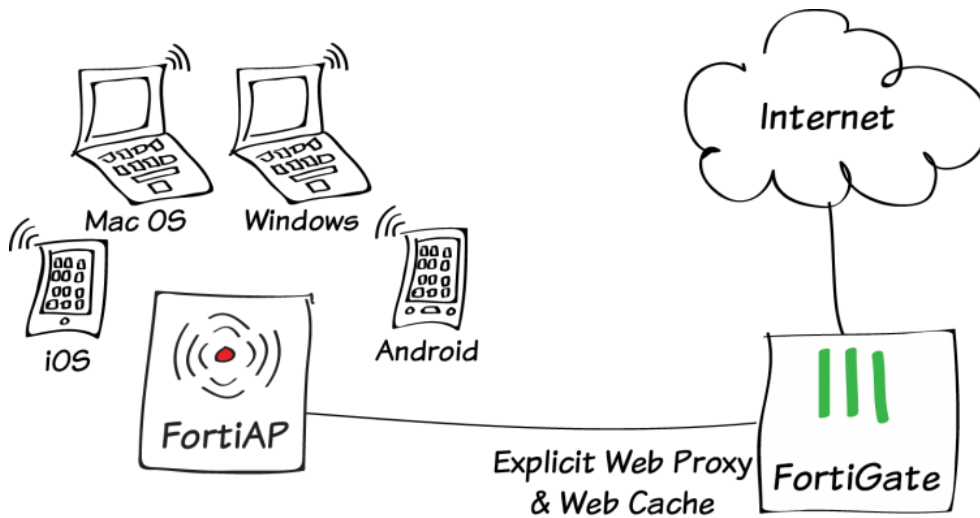
Notice that in both cases FortiAP-2 is listed on *backhaul-ssid* as a client of FortiAP-1.

| SSID          | FortiAP       | User   | IP          | Device            | Channel | Bandwidth Tx/Rx | Signal Strength/Noise | Signal   |
|---------------|---------------|--------|-------------|-------------------|---------|-----------------|-----------------------|----------|
| example-staff | FortiAP-2 (1) | rgreen | 10.10.12.2  | 08:fd:0e:ff:0c:56 | 11      | 3.19 Mbps       | 44 dB                 | ████████ |
| backhaul-ssid | FortiAP-1 (2) |        | 192.168.1.4 | 7a:5b:0e:89:1b:75 | 153     | 0 bps           | 44 dB                 | ████████ |

| SSID          | FortiAP       | User   | IP          | Device            | Channel | Bandwidth Tx/Rx | Signal Strength/Noise | Signal   |
|---------------|---------------|--------|-------------|-------------------|---------|-----------------|-----------------------|----------|
| example-staff | FortiAP-1 (1) | rgreen | 10.10.12.2  | 08:fd:0e:ff:0c:56 | 11      | 3.14 Mbps       | 0 dB                  | ████████ |
| backhaul-ssid | FortiAP-2 (2) |        | 192.168.1.4 | 7a:5b:0e:89:1b:75 | 153     | 0 bps           | 44 dB                 | ████████ |

For further reading, check out **Wireless Mesh** in the **FortiOS 5.2 Handbook**.

# Explicit proxy with web caching



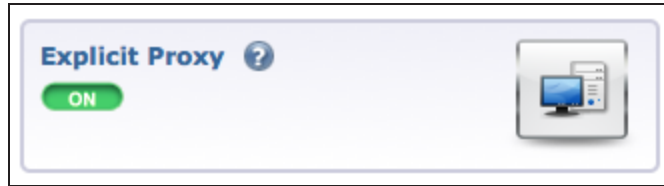
In this example, you will add explicit proxy with web caching to your wireless network.

All devices on the wireless network will be required to connect to the proxy at port 8080 before they can browse web pages on the Internet. WAN Optimization web caching is added to reduce the amount of Internet bandwidth used and improve web browsing performance.

A video of this recipe is available [here](#).

## 1. Enabling WAN Optimization and configuring the explicit web proxy for the wireless interface

Go to **System > Config > Features**.  
Ensure that **Explicit Proxy** and **WAN Opt & Cache** are enabled.



Go to **System > Network > Interfaces**,  
edit the wireless interface and select  
**Enable Explicit Web Proxy**.

|                                       |                                     |
|---------------------------------------|-------------------------------------|
| Enable Explicit Web Proxy             | <input checked="" type="checkbox"/> |
| Listen for RADIUS Accounting Messages | <input type="checkbox"/>            |
| Secondary IP Address                  | <input type="checkbox"/>            |

Go to **System > Network > Explicit Proxy**. Select **Enable Explicit Web Proxy** for HTTP/HTTPS. Make sure that **Default Firewall Policy Action** is set to **Deny**.

▼ Explicit Web Proxy Options



Enable Explicit Web Proxy

☒ HTTP / HTTPS ☐ FTP ☐ PAC

Enable IPv6 Explicit Proxy

☐

Listen on Interfaces

mgmt2  

HTTP Port

HTTPS Port

(0 to use HTTP port)


FTP Port

(0 to use HTTP port)

PAC Port

(0 to use HTTP port)

PAC File Content



Proxy FQDN


Max HTTP request length

Kb

Max HTTP message length

Kb

Unknown HTTP version



Realm

Default Firewall Policy Action

☐ Accept ☒ Deny

## 2. Adding an explicit web proxy policy

Go to **Policy & Objects > Policy > Explicit Proxy** and create a new policy. Set **Explicit Proxy Type** to **Web** and the **Outgoing Interface** to the Internet-facing interface.

Explicit Proxy Type


☒ Web ☐ FTP

Enabled On

Internal-WiFi 

Source Address

 all



Outgoing Interface

wan1




Destination Address

 all




Schedule

 always



Action

 ACCEPT



Turn on **Web Cache**.

ON

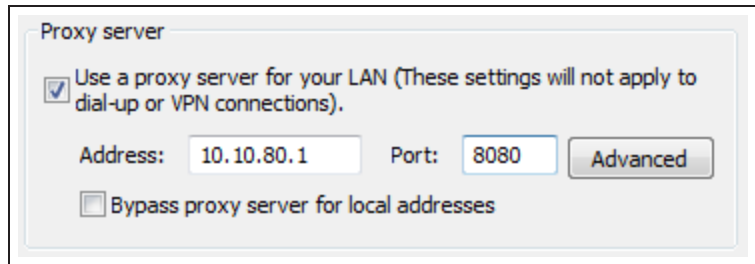
Web Cache

### 3. Configuring devices on the wireless network to use the web proxy

To use the web proxy, all devices on the wireless network must be configured to use the explicit proxy server. The IP address of the server is the IP address of the FortiGate's wireless interface (in the example, *10.10.80.1*) and the port is 8080. Some browsers may have to be configured to use the device's proxy settings.

#### Windows Vista/7/8:

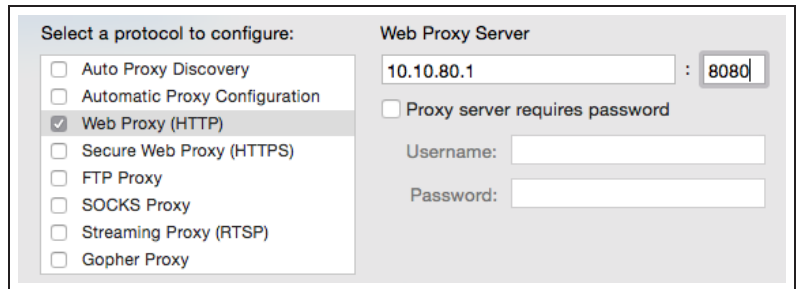
Open **Internet Properties**. Go to **Connections > LAN Settings** and enable and configure the **Proxy Server**.



The screenshot shows the 'Proxy server' tab in the Windows Internet Properties dialog. The checkbox 'Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)' is checked. The 'Address' field is set to '10.10.80.1' and the 'Port' field is set to '8080'. There is an 'Advanced' button to the right of the port field. Below these fields, the checkbox 'Bypass proxy server for local addresses' is unchecked.

#### Mac OS X:

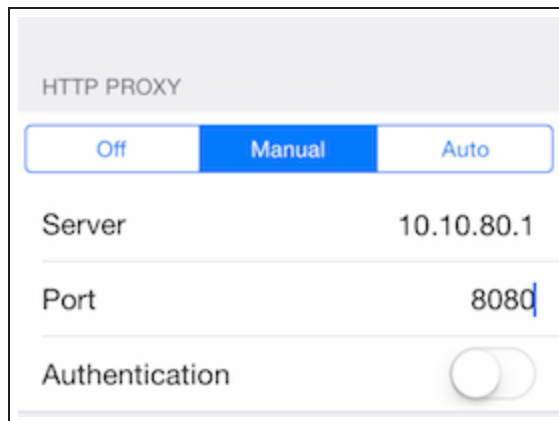
Open **Network Preferences > Wi-Fi > Advanced > Proxies**. Select **Web Proxy (HTTP)** and configure the proxy settings.



The screenshot shows the 'Proxies' tab in the Mac OS X Network Preferences window. Under 'Select a protocol to configure:', 'Web Proxy (HTTP)' is selected with a checked checkbox. Other protocols like 'Auto Proxy Discovery', 'Automatic Proxy Configuration', 'Secure Web Proxy (HTTPS)', 'FTP Proxy', 'SOCKS Proxy', 'Streaming Proxy (RTSP)', and 'Gopher Proxy' are unchecked. On the right, under 'Web Proxy Server', the address '10.10.80.1' is entered in the first field and '8080' is entered in the second field. The checkbox 'Proxy server requires password' is unchecked. Below this, there are empty input fields for 'Username:' and 'Password:'.

#### iOS:

Go to **Settings > Wi-Fi**. Edit the wireless network. Scroll down to **HTTP PROXY** select **Manual** and configure the proxy settings.



The screenshot shows the 'HTTP PROXY' settings in the iOS Settings app. At the top, there are three buttons: 'Off', 'Manual', and 'Auto'. The 'Manual' button is selected and highlighted in blue. Below the buttons, the 'Server' is set to '10.10.80.1' and the 'Port' is set to '8080'. At the bottom, there is an 'Authentication' section with a toggle switch that is currently turned off.

Android:

In WiFi network connection settings, edit the wireless network. Select **Show advanced options**, configure a **Manual** proxy and enter the proxy settings.

Proxy

Manual

HTTP proxy used by browser but may not be used by other applications

Proxy hostname

10.10.80.1

Proxy port

8080

4. Force HTTP and HTTPS traffic to use the Web Proxy

Block HTTP and Replace...HTTPS access to the Internet from the wireless network so that the only path to the Internet is through the explicit proxy. You can edit or delete policies that allow HTTP or HTTPS access. You can also add a policy to the top of the list that **Denies** HTTP and HTTPS traffic.

|                     |                                |     |
|---------------------|--------------------------------|-----|
| Incoming Interface  | Internal-WiFi (SSID: fortinet) | +   |
| Source Address      | all                            | +   |
| Source User(s)      | Click to add...                |     |
| Source Device Type  | Click to add...                |     |
| Outgoing Interface  | wan1                           | +   |
| Destination Address | all                            | +   |
| Schedule            | always                         |     |
| Service             | HTTP                           | X + |
|                     | HTTPS                          | X   |
| Action              | DENY                           |     |

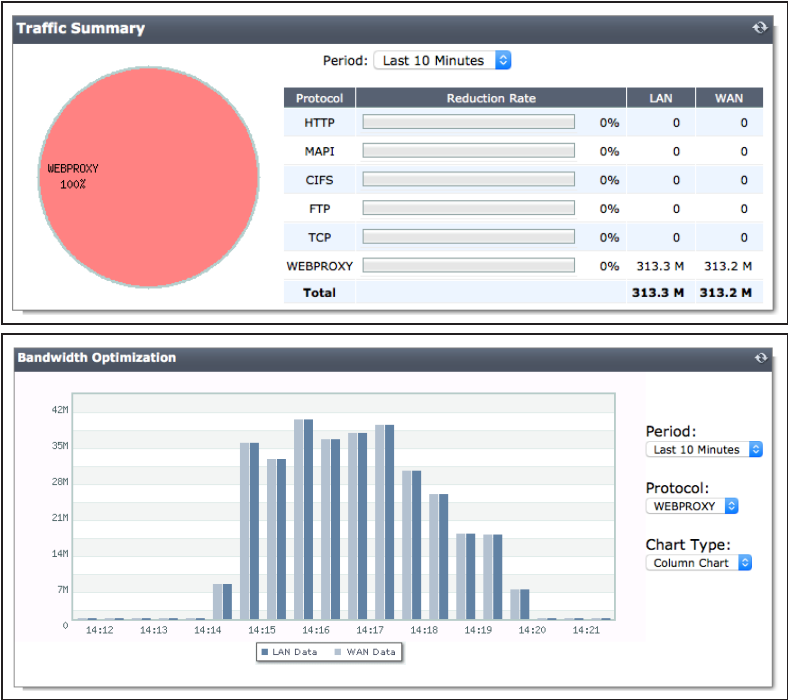


# 5. Results

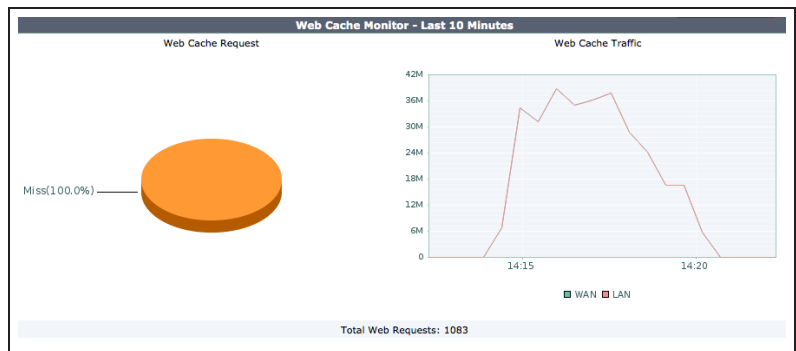
To confirm that the proxy is processing traffic, attempt to connect to the Internet from the Wireless network using a device that has not been configured to connect to the proxy. Access should be blocked.

Configure the device to use the proxy.  
You should now be able to connect to the Internet.

Go to **WAN Opt. & Cache > Monitor > WAN Opt. Monitor** to view **WEBPROXY** traffic in the **Traffic Summary**. Check the **Bandwidth Optimization** graph for **WEBPROXY** traffic.

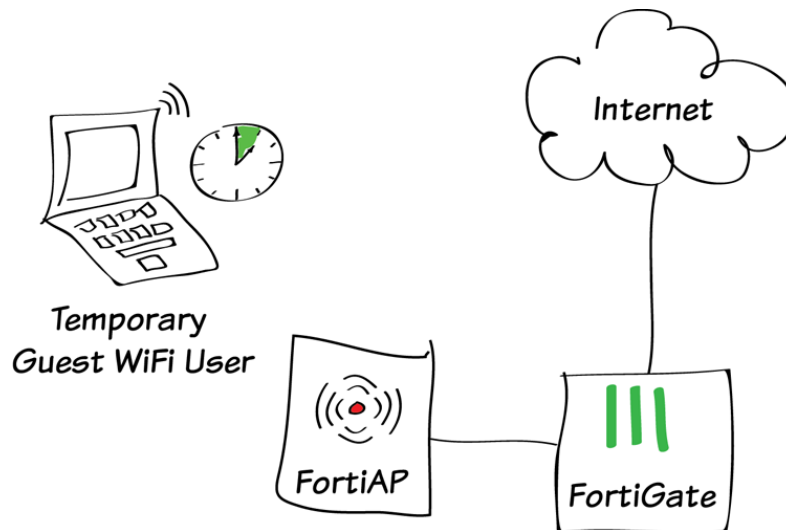


Go to **WAN Opt. & Cache > Monitor > Cache Monitor** to view web caching activity.



For further reading, check out [The FortiGate explicit web proxy in the FortiOS 5.2 Handbook](#).

# Guest WiFi accounts



In this example, a guest user account will be created to allow temporary wireless access to the Internet. Access will only be allowed using HTTP, HTTPS, and DNS protocols.

In this example, a FortiAP in Tunnel mode is used to provide wireless access to guests.

If you have not already set up a wireless network, see [Setting up WiFi with FortiAP](#).

A video of this recipe is available [here](#).

## 1. Creating a WiFi guest user group

Go to **User & Device > User > User Groups** and create a new group.

Set **Type** to **Guest**. Set **User ID** to **Email**, ensure that **Password** is set to **Auto-Generate**, and set **Expiry Type** to **After first login**. Leave **Default Expiry Time** set to **4 Hours**.

The screenshot shows the configuration for a new user group named 'WiFi\_guests'. The 'Type' is set to 'Guest'. The 'User ID' is 'Email', 'Password' is 'Auto-Generate', and 'Expiry Type' is 'After first login'. The 'Default Expiry Time' is '4 Hours'. There are checkboxes for 'Enable Batch Guest Account Creation', 'Enable Name', 'Enable Sponsor', 'Enable Company', 'Enable Email', 'Enable SMS', 'Required', and 'Maximum Accounts'.

|  |   |
|--|---|
| Name   | WiFi_guests   |
| Type   | <input type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input checked="" type="radio"/> Guest <input type="radio"/> RADIUS Single Sign-On (RSSO) |
| <input type="checkbox"/> Enable Batch Guest Account Creation |   |
| User ID  | Email   |
| Password   | Auto-Generate   |
| Expiry Type  | After first login   |
| Default Expiry Time  | 4   |
|  | Hours   |
| Maximum Accounts   | <input type="checkbox"/>  |
| <input type="checkbox"/> Enable Name                         |   |
| <input checked="" type="checkbox"/> Enable Sponsor           | <input type="checkbox"/> Required   |
| <input checked="" type="checkbox"/> Enable Company           | <input type="checkbox"/> Required   |
| <input checked="" type="checkbox"/> Enable Email             |   |
| <input type="checkbox"/> Enable SMS                          |   |

## 2. Creating a guest SSID that uses Captive Portal

Go to **Wireless Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**. Assign an **IP/Network Mask** to the interface and enable **DHCP server**. Under **WiFi Settings**, set **Security Mode** to **Captive Portal** and **User Group(s)** to the WiFi guest user group.

The screenshot shows the configuration for a new WiFi SSID named 'WiFi\_guests'. The 'Type' is 'WiFi SSID' and 'Traffic Mode' is 'Tunnel to Wireless Controller'. The 'IP/Network Mask' is '10.10.80.1/255.255.255.0'. The 'Administrative Access' section has checkboxes for HTTPS, PING, HTTP, FMG-Access, SSH, SNMP, and FCT-Access. The 'DHCP Server' is enabled, and the 'Address Range' is set to '10.10.80.2' to '10.10.80.254'. The 'Netmask' is '255.255.255.0'. The 'Default Gateway' is 'Same as Interface IP' and the 'DNS Server' is 'Same as System DNS'. The 'WiFi Settings' section shows 'SSID' as 'guest', 'Security Mode' as 'Captive Portal', 'Portal Type' as 'Authentication', 'Authentication Portal' as 'Local', and 'User Groups' as 'WiFi\_guests'.

| Interface Name        | WiFi_guests  |             |        |            |              |
|-----------------------|--|-------------|--------|------------|--------------|
| Type                  | WiFi SSID  |             |        |            |              |
| Traffic Mode          | Tunnel to Wireless Controller  |             |        |            |              |
| IP/Network Mask       | 10.10.80.1/255.255.255.0   |             |        |            |              |
| Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access |             |        |            |              |
| DHCP Server           | <input checked="" type="checkbox"/> Enable   |             |        |            |              |
| Address Range         | <table border="1"><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.80.2</td><td>10.10.80.254</td></tr></tbody></table>  | Starting IP | End IP | 10.10.80.2 | 10.10.80.254 |
| Starting IP           | End IP   |             |        |            |              |
| 10.10.80.2            | 10.10.80.254   |             |        |            |              |
| Netmask               | 255.255.255.0  |             |        |            |              |
| Default Gateway       | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |            |              |
| DNS Server            | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify  |             |        |            |              |
| Advanced...           |  |             |        |            |              |
| WiFi Settings         |  |             |        |            |              |
| SSID                  | guest  |             |        |            |              |
| Security Mode         | Captive Portal   |             |        |            |              |
| Portal Type           | <input checked="" type="radio"/> Authentication <input type="radio"/> Disclaimer + Authentication <input type="radio"/> Disclaimer Only <input type="radio"/> Email Collection   |             |        |            |              |
| Authentication Portal | <input checked="" type="radio"/> Local <input type="radio"/> External  |             |        |            |              |
| User Groups           | WiFi_guests  |             |        |            |              |

Go to **Wireless Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model (in the example, FortiAP-11C).

Set the FortiAP to broadcast the new **SSID**.

The screenshot shows the FortiAP Profile configuration page. The 'SSID' field is set to 'WiFi\_guests (SSID: guest)'.

|      |                           |
|------|---------------------------|
| SSID | WiFi_guests (SSID: guest) |
|------|---------------------------|

### 3. Creating a security policy for WiFi guests

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the guest SSID, **Source User(s)** to the WiFi guest user group, the **Outgoing Interface** to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.

|                     |                           |
|---------------------|---------------------------|
| Incoming Interface  | WiFi_guests (SSID: guest) |
| Source Address      | all                       |
| Source User(s)      | WiFi_guests               |
| Source Device Type  | Click to add...           |
| Outgoing Interface  | wan1                      |
| Destination Address | all                       |
| Schedule            | always                    |
| Service             | HTTP<br>HTTPS<br>DNS      |
| Action              | ACCEPT                    |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

### 4. Creating a guest user account

Go to **User & Device > User > Guest Management** and create a new account.

Set **Email** to the user's email address (in the example, *ballen@example.com*). To test the account, set **Expiration** to **5 Minutes**.

|            |   |  |
|------------|---|--|
| User ID    | Use Email Address                               |  |
| Password   | Auto Generated                                  |  |
| Sponsor    | <input type="text"/>                            | Optional                                 |
| Company    | <input type="text"/>                            | Optional                                 |
| Email      | <input type="text" value="ballen@example.com"/> |  |
| Expiration | <input type="text" value="5"/>                  | Minutes <input type="button" value="v"/> |

After you select **OK**, a **User Created Successfully** notice will appear, listing the generated Password. This password can then be printed or emailed to the guest user.

**User Created Successfully**

User ID ballen@example.com

Password qa3q3z

Email ballen@example.com

Expiration 0:05:00

Send

## (Optional) 5. Creating a restricted admin account for guest user management

To make it easier for guest accounts to be created, an admin account can be made that is only used for guest user management. In this example, the account is made for use by the receptionist.

Go to **System > Admin > Administrators** and create a new account.

Set **Type** to **Regular** and set a **Password**. Select **Restrict to Provision Guest Accounts** and set **Guest Groups** to the WiFi guest user group.

Administrator

Reception

Type

☒ Regular ☐ Remote ☐ PKI

Password

.....

Confirm Password

.....

Comments

Write a comment...

0/255

Contact Info

☐ Email Address

☐ SMS

☒ FortiGuard Messaging Service ☐ Custom

Country/Region 

Click to add...

Phone Number

☐ Enable Two-factor Authentication

☐ Restrict this Administrator Login from Trusted Hosts Only

☒ Restrict to Provision Guest Accounts

Guest Groups 

WiFi\_guests

Sign in to the FortiGate using this account. You will only be able to see the menu for **Guest User Management**.

Guest Groups: WiFi\_guests

**Guest User Management**

Logout

Create New

Edit

Delete

Purge

Print

Send

Refresh

User ID

expires

ballen@example.com

5 Minutes after first login

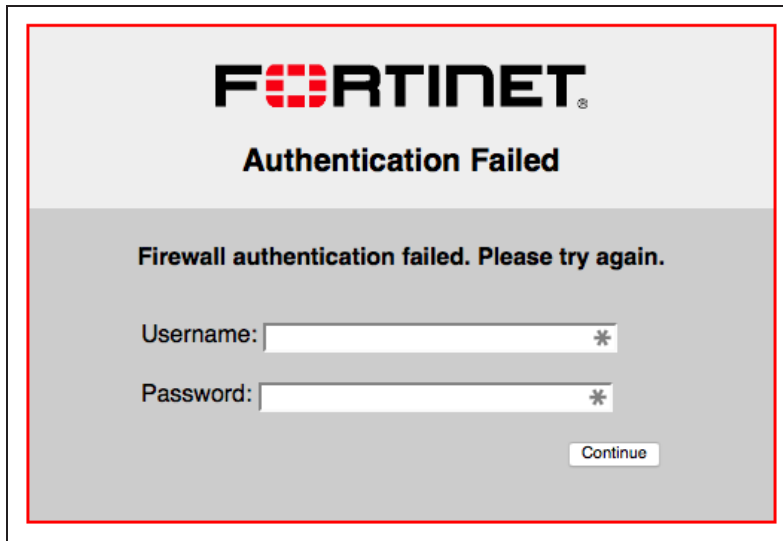
## 6. Results

On a PC, connect to the guest SSID. When the authentication screen appears, log in using the guest user's credentials. You will be able to connect to the Internet.



The image shows a Fortinet authentication screen. At the top, the Fortinet logo is displayed in black with a red square icon. Below the logo, the text "Authentication Required" is centered. A message "Please enter your username and password to continue." is displayed. There are two input fields: "Username:" with the value "ballen@example.com" and "Password:" with masked characters ".....". A "Continue" button is located at the bottom right.

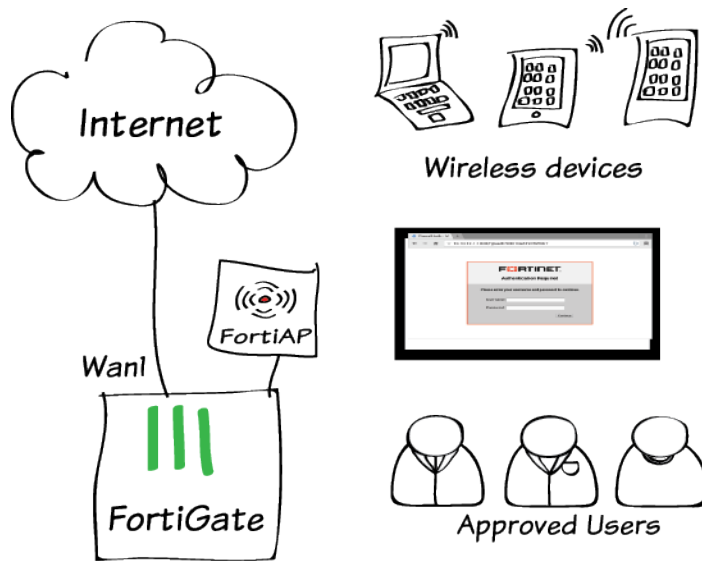
Five minutes after the initial login, the user account will expire and you will no longer be able to log in using those credentials.



The image shows a Fortinet authentication screen with the title "Authentication Failed". Below the Fortinet logo, the text "Authentication Failed" is centered. A message "Firewall authentication failed. Please try again." is displayed. There are two input fields: "Username:" and "Password:", both with masked characters "\*\*\*\*\*". A "Continue" button is located at the bottom right.

For further reading, check out [Managing Guest Access](#) in the [FortiOS 5.2 Handbook](#).

# Captive portal WiFi access control



In this example, your employees can log on to your Wi-Fi network through a captive portal.

Captive portals are often used for public Wi-Fi networks where you want Wi-Fi users to respond to a disclaimer. Captive portals can also be used to provide unlimited access to open Wi-Fi networks.

As shown in this example, captive portals can also be used as the authentication method for restricting access to a wireless network. Some users may find it more intuitive to add their account information to a captive portal web page instead of entering their user name and password into a wireless network configuration.

A video of this recipe is available [here](#).



# 1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.

✓ User Type

2 Login Credentials

3 Contact Info

4 Extra Info

User Name

rgreen

Password

••••••••

< Back

Next >

Cancel

# 2. Create a user group

Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

Name

employees

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest

Members

gbrown

×

+

rgreen

×

# 3. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

Interface Name

example-wifi

Type

WiFi SSID

Traffic Mode

Tunnel to Wireless Controller

IP/Network Mask

10.10.12.1/255.255.255.0

IPv6 Address/Prefix

::/0

Configure DHCP addressing for clients.

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.10.12.2  | 10.10.12.254 |

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

▶ Advanced...

Configure Captive Portal authentication using the *employees* user group.

WiFi Settings

SSID

example-staff

Security Mode

Captive Portal

Portal Type

☒ Authentication ☐ Disclaimer + Authentication

Authentication Portal

☒ Local ☐ External

User Groups

employees

Exempt List

Click to add...

Customize Portal Messages

[Login Page](#)

Redirect after Captive Portal

☒ Original Request ☐ Specific URL

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

Optional VLAN ID

0

#### 4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.

New Address

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

example-wifi-net

Type

Subnet

Subnet / IP Range

10.10.12.0/24

Interface

example-wifi (SSID: example-staff)

Visibility

☒

Comments

OK

Cancel

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet. Select the *employees* user group as permitted **Source Users**.

Incoming Interface

example-wifi (SSID: example-staff)

Source Address

example-wifi-net

Source User(s)

employees

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

## 5. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**.  
Configure an interface dedicated to extension devices and assign it an IP address.

Addressing mode

☐ Manual ☐ DHCP ☐ PPPoE ☒ Dedicated to Extension Device

IP/Network Mask

10.11.12.1/255.255.255.0

Connected Devices

None

Connect the FortiAP unit to the interface and go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

| Create New | Edit             | Delete | Refresh       | Display By           | AP                     | Radio                    | Managed FortiAPs | 1/64            |
|------------|------------------|--------|---------------|----------------------|------------------------|--------------------------|------------------|-----------------|
| Mesh       | Access Point     | State  | Connected Via | SSIDs                | Channel                | Clients                  | OS Version       | FortiAP Profile |
|            | FP221C3X14019926 |        | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |                  | FAP221C-default |

The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

*The FortiAP may not appear for a minute or two.*

Highlight the FortiAP unit on the list and select **Authorize**.

| <div>Create New Edit Delete Authorize Refresh</div> |                  |             |                       | Display By <div>AP Radio</div> |                        | Managed FortiAPs <div>1/64</div> |            |                 |
|---|------------------|-------------|-----------------------|--------------------------------|------------------------|----------------------------------|------------|-----------------|
| Mesh  | Access Point     | State       | Connected Via         | SSIDs                          | Channel                | Clients                          | OS Version | FortiAP Profile |
| .   | FP221C3X14019926 | <div></div> | <div>10.11.12.2</div> | Radio 1:<br>Radio 2:           | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0         |            | FAP221C-default |

A grey check mark is now shown beside the FortiAP, showing that it is authorized but not yet online.

| Create New | Edit             | Delete | Refresh       | Display By           | AP                     | Radio                    | Managed FortiAPs | 1/64            |
|------------|------------------|--------|---------------|----------------------|------------------------|--------------------------|------------------|-----------------|
| Mesh       | Access Point     | State  | Connected Via | SSIDs                | Channel                | Clients                  | OS Version       | FortiAP Profile |
|            | FP221C3X14019926 |        | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |                  | FAP221C-default |

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

Enable **Radio Resource Provision**.

Select your SSID.

Radio 2

Mode

☐ Disable ☒ Access Point

Spectrum Analysis

☐

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

5GHz 802.11ac/n/a

Select Channel Width

20MHz

Channel

☒ 36 ☐ 40 ☒ 44 ☐ 48 ☒ 149 ☐ 153 ☒ 157 ☐ 161 ☒ 165

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

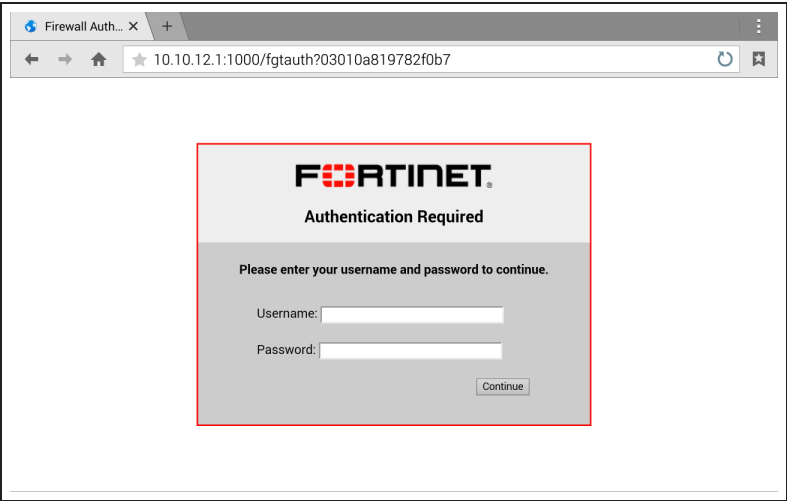
SSID

example-wifi (SSID: exa...

X

## 6. Results

The user's device shows the WiFi network as "open" and associates with it without requesting credentials. The first time that a wireless user attempts to use a web browser, the captive portal login screen is displayed. Users who are members of the *employees* group can log on using their username and password and proceed to access the wireless network.

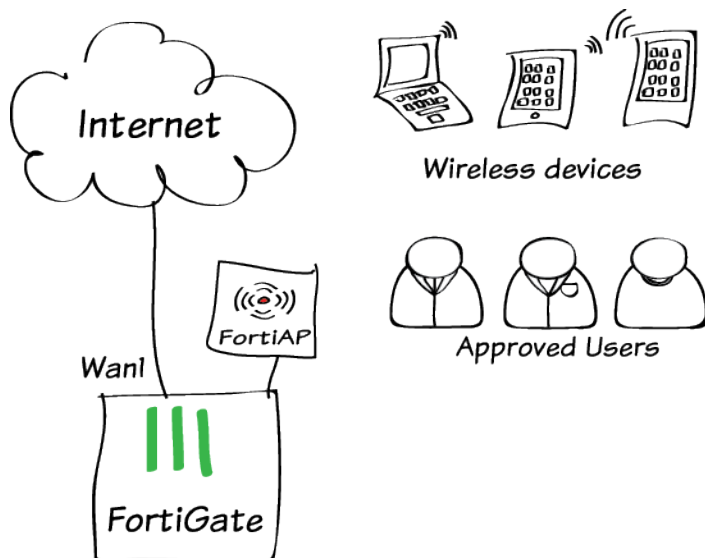


Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

| SSID          | FortiAP              | User   | IP         | Device            | Channel | Bandwidth Tx/Rx | Signal Strength |
|---------------|----------------------|--------|------------|-------------------|---------|-----------------|-----------------|
| example-staff | FP221C3X14019926 (2) | rgreen | 10.10.12.2 | 08:fd:0e:ff:0c:56 | 165     | 76.02 Kbps      | 50 dB           |

For further reading, check out [Captive portals](#) in the [FortiOS 5.2 Handbook](#).

# WPA2 WiFi access control



In this example, you will improve your WiFi security with WPA2 enterprise authentication.

In the [Setting up WiFi with FortiAP](#) recipe, you set up a WiFi network with a single pre-shared key. In this example, there is no longer a pre-shared key that could fall into the wrong hands, or that needs to be changed if someone leaves the company. Each user has an individual user account and password, and accounts can be added or removed later as needed.

This example shows how to authenticate local FortiGate users. You can also integrate WPA2 security with most 3rd party authentication solutions including RADIUS.

## 1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.

The screenshot shows the 'User Definition' form at the 'Login Credentials' step. The progress bar at the top indicates four steps: 1. User Type (checked), 2. Login Credentials (active), 3. Contact Info, and 4. Extra Info. The 'User Name' field contains 'rgreen'. The 'Password' field is masked with dots. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

## 2. Create a user group

Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

The screenshot shows the 'User Groups' form. The 'Name' field contains 'employees'. The 'Type' field has three radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest'. The 'Members' section shows a list of users: 'gbrown' and 'rgreen', each with a remove icon (X) and an add icon (+).

## 3. Create the SSID and enable the WiFi radio

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

The screenshot shows the 'WiFi Network > SSID' configuration form. The 'Interface Name' field contains 'example-wifi'. The 'Type' dropdown is set to 'WiFi SSID'. The 'Traffic Mode' dropdown is set to 'Tunnel to Wireless Controller'. The 'IP/Network Mask' field contains '10.10.12.1/255.255.255.0'. The 'IPv6 Address/Prefix' field contains '::/0'.

Configure DHCP addressing for clients.

The screenshot shows the 'DHCP Server' configuration form. The 'Enable' checkbox is checked. The 'Address Range' section shows a table with 'Starting IP' and 'End IP' columns. The 'Netmask' field contains '255.255.255.0'. The 'Default Gateway' and 'DNS Server' fields have radio buttons for 'Same as Interface IP' and 'Specify'. The 'Advanced...' link is visible at the bottom.

| Starting IP | End IP       |
|-------------|--------------|
| 10.10.12.2  | 10.10.12.254 |

Configure WPA2-Enterprise authentication using the *employees* user group.

WiFi Settings

SSID

example-staff

Security Mode

WPA2 Enterprise

Authentication

Local

RADIUS Server

employees

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Optional VLAN ID

0

#### 4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.

New Address

Category

Address

IPv6 Address

Multicast Address

Name

example-wifi-net

Type

Subnet

Subnet / IP Range

10.10.12.0/24

Interface

example-wifi (SSID: example-staff)

Visibility

☒

Comments

OK

Cancel

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet.

Incoming Interface

example-wifi (SSID: example-staff)

Source Address

example-wifi-net

Source User(s)

employees

Source Device Type

Click to add...

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

# Results

Users who are members of the *employees* group can log on to the WiFi network using their username and password.

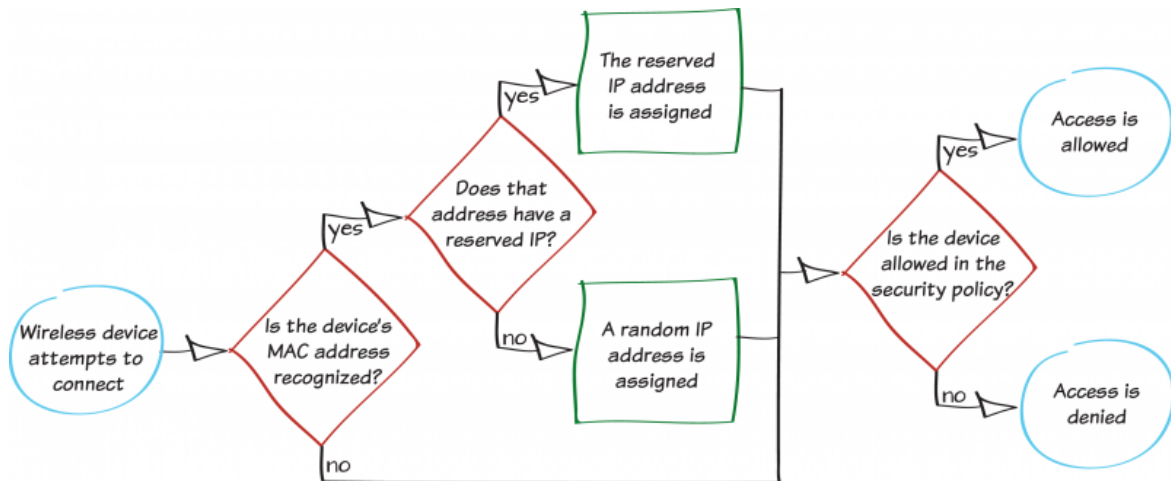
Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

| SSID          | FortiAP              | User   | IP         | Device            | Channel | Bandwidth Tx/Rx | Signal Strength |
|---------------|----------------------|--------|------------|-------------------|---------|-----------------|-----------------|
| example-staff | FP221C3X14019926 (2) | rgreen | 10.10.12.2 | 08:fd:0e:ff:0c:56 | 165     | 76.02 Kbps      | 50 dB           |

For further reading, check out [Deploying Wireless Networks](#) in the [FortiOS 5.2 Handbook](#).



# MAC access control



In this example, you will add device definitions to your FortiGate using Media Access Control (MAC) addresses. These definitions are then used to determine which devices can access the wireless network.

By using a MAC address for identification, you will also be able to assign a reserved IP for exclusive use by the device when it connects to the wireless network.

**Warning:** Since MAC addresses can be easily spoofed, using MAC access control should not be considered a security measure.

A video of this recipe is available [here](#).

## 1. Finding the MAC address of a device

The instructions below were written for the most recent OS versions. Older versions may use different methods.

### For Windows devices:

Open the command prompt and type  
`ipconfig /all`

This output displays configuration information for all of your network connections. Look for the information about the wireless adapter and take note of the **Physical Address**.

```
Wireless LAN adapter Wireless Network Connection 3:  
    Connection-specific DNS Suffix  . :  
    Description . . . . . : 802.11n USB Wireless LAN Card  
    Physical Address. . . . . : C8-3A-35-C4-2F-B7  
    DHCP Enabled. . . . . : Yes
```

### For Mac OS X devices:

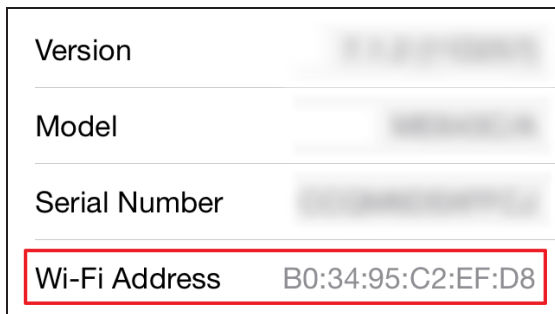
Open **Terminal** and type `ifconfig en1 | grep ether`

Take note of the displayed MAC address.

```
drsr:~ % ifconfig en1 | grep ether  
ether c8:bc:c8:de:26:3c
```

### For iOS devices:

Open **Settings > General** and take note of the **Wi-Fi Address**.



For Android devices:

Open **Settings > More > About Device > Status** and take note of the **Wi-Fi MAC** address.



## 2. Defining a device using its MAC address

Go to **User & Device > Device > Device Definitions** and create a new device definition.

Set MAC Address to the address of the device and set the other fields as required. In the example, a device definition is created for an iPhone with the MAC Address B0:34:95:C2:EF:D8.

|                 |   |
|-----------------|---|
| Alias           | <input type="text" value="iPhone"/>                   |
| MAC Address     | <input type="text" value="B0:34:95:C2:EF:D8"/>        |
| Additional MACs | <input type="button" value="Click to add..."/>        |
| Device Type     | <input type="text" value="iPhone"/>                   |
| Custom Groups   | <input type="text" value="None"/>                     |
| Comments        | <input type="text" value="Write a comment..."/> 0/255 |

The new definition will now appear in your device list.

*If you have enabled device identification on the wireless interface, device definitions will be created automatically. You can then use MAC addresses to identify which device a definition refers to.*

| Status  | Device     | OS              | IP Address |
|---------|------------|-----------------|------------|
| Online  | My-Desktop | Windows         | 10.10.80.3 |
| Offline | My-Android | Android / 2.2.2 | 10.10.80.4 |
| Offline | My-iPhone  | iPod / iOS      | 10.10.80.7 |
| Offline | My-Netbook | Windows         | 10.10.80.5 |
| Offline | My-Printer | Linux           | 10.10.80.6 |

### 3. Creating a device group

Go to **User & Device > Device > Device Groups** and create a new group.

Add the new device to the **Members** list.

|          |  |
|----------|--|
| Name     | <input type="text" value="wifi-access"/>   |
| Members  | <div><div></div> My-iPhone <div>X</div> <div>+</div></div>                             |
| Comments | <div><div><input type="text" value="Write a comment..."/></div> <div>0/255</div></div> |

### 4. Reserving an IP address for the device

Go to **System > Network > Interfaces** and edit the wireless interface.

*If the FortiAP is in bridge mode, you will need to edit the internal interface.*

Under **DHCP Server**, expand **Advanced**. Create a new entry in the **MAC Reservation + Access Control** list that reserves an IP address within the DHCP range for the device's MAC address.

|          |  |
|----------|--|
| Name     | <input type="text" value="wifi-access"/>   |
| Members  | <div><div></div> My-iPhone <div>X</div> <div>+</div></div>                             |
| Comments | <div><div><input type="text" value="Write a comment..."/></div> <div>0/255</div></div> |

### 5. Creating a security policy for wireless traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your wireless interface, **Source Device Type** to the device group, and **Outgoing Interface** to the Internet-facing interface.

Ensure that **NAT** is turned on.

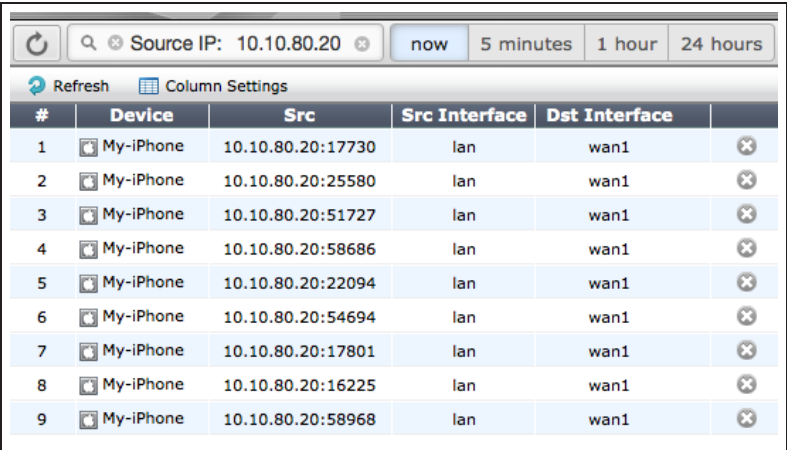
|  |  |
|--|--|
| Incoming Interface   | <div>wifi (SSID: NAMAAH) <div>+</div></div>                  |
| Source Address   | <div><div></div> all <div>+</div></div>                      |
| Source User(s)   | <div>Click to add...</div>                                   |
| Source Device Type   | <div><div></div> wifi-access <div>X</div> <div>+</div></div> |
| Outgoing Interface   | <div>any <div>+</div></div>                                  |
| Destination Address  | <div><div></div> all <div>+</div></div>                      |
| Schedule   | <div><div></div> always <div>+</div></div>                   |
| Service  | <div><div></div> ALL <div>+</div></div>                      |
| Action   | <div><div></div> ACCEPT <div>+</div></div>                   |
| <b>Firewall / Network Options</b>  |  |
| <div><div>ON</div> NAT</div>   |  |
| <div><div><div><input checked="" type="radio"/> Use Destination Interface Address</div> <div><input type="checkbox"/> Fixed Port</div></div></div> |  |
| <div><div><div><input type="radio"/> Use Dynamic IP Pool</div> <div><input type="text" value="Click to add..."/></div></div></div>                 |  |

## 6. Results

Connect to the wireless network with a device that is a member of the device group. The device should be able to connect and allow Internet access.

Connection attempts from a device that is not a group member will fail.

Go to **System > FortiView > All Sessions** and view the results for now. Filter the results using the reserved **Source IP** (in the example, 10.10.80.20), to see that it is being used exclusively by the wireless device.

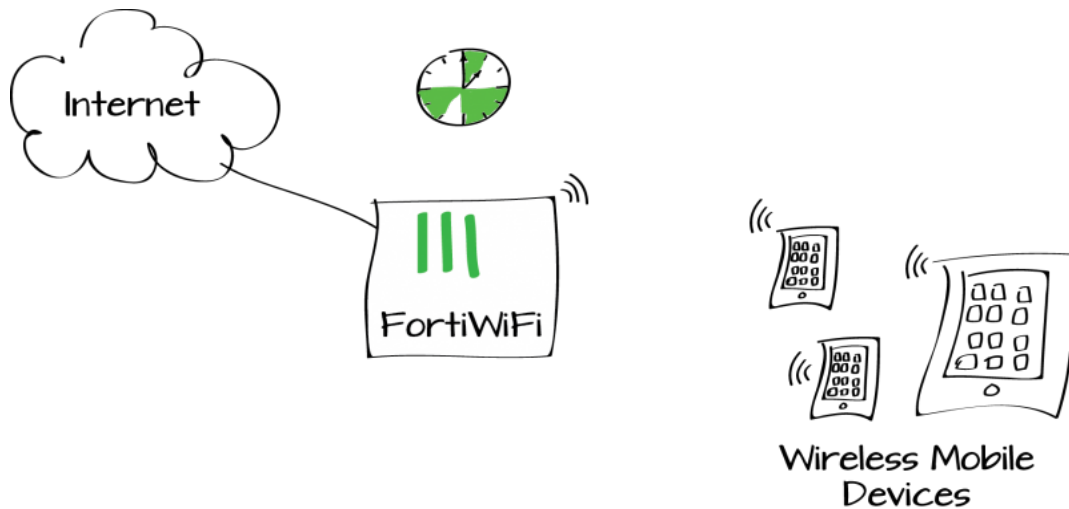


The screenshot shows the FortiView 'All Sessions' page. At the top, there is a search bar with 'Source IP: 10.10.80.20' and a 'now' filter. Below the search bar are 'Refresh' and 'Column Settings' buttons. The main table has columns: '#', 'Device', 'Src', 'Src Interface', 'Dst Interface', and a status icon. It lists 9 sessions, all from 'My-iPhone' devices with source IP 10.10.80.20, connected to 'lan' and destined for 'wan1'. Each session has a red 'X' icon in the status column, indicating a failed connection attempt.

| # | Device    | Src               | Src Interface | Dst Interface |   |
|---|-----------|-------------------|---------------|---------------|---|
| 1 | My-iPhone | 10.10.80.20:17730 | lan           | wan1          | × |
| 2 | My-iPhone | 10.10.80.20:25580 | lan           | wan1          | × |
| 3 | My-iPhone | 10.10.80.20:51727 | lan           | wan1          | × |
| 4 | My-iPhone | 10.10.80.20:58686 | lan           | wan1          | × |
| 5 | My-iPhone | 10.10.80.20:22094 | lan           | wan1          | × |
| 6 | My-iPhone | 10.10.80.20:54694 | lan           | wan1          | × |
| 7 | My-iPhone | 10.10.80.20:17801 | lan           | wan1          | × |
| 8 | My-iPhone | 10.10.80.20:16225 | lan           | wan1          | × |
| 9 | My-iPhone | 10.10.80.20:58968 | lan           | wan1          | × |

For further reading, check out [Managing "bring your own device"](#) in the [FortiOS 5.2 Handbook](#).

# BYOD scheduling



In this example, a school blocks Internet access to mobile devices during class time (9am - 12pm and 1pm - 3pm).

This recipe shows how to use a schedule group and a BYOD device policy to permit mobile device Internet access before and after class time and during lunch. The school is open from 7am to 6pm.

*In this example a FortiWiFi unit provides the wireless network. The steps are the same if the wireless network is provided by FortiAP with a FortiGate as a wireless controller.*

A video of this recipe is available [here](#).

# 1. Creating schedules and a schedule group

Go to **Policy & Objects > Objects > Schedules**. Create recurring schedules for the before class (7-9 am), lunch (12-1 pm), and after class (3-6 pm) periods.

New Schedule

Type

☒ Recurring

☐ One-time

Name

before class

Days

☐ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☐ Saturday

Start Time

Hour

7

Minute

0

?

Stop Time

Hour

9

Minute

0

OK

Cancel

New Schedule

Type

☒ Recurring

☐ One-time

Name

lunch

Days

☐ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☐ Saturday

Start Time

Hour

12

Minute

0

?

Stop Time

Hour

13

Minute

0

OK

Cancel

New Schedule

Type

☒ Recurring

☐ One-time

Name

after class

Days

☐ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☒ Thursday

☒ Friday

☐ Saturday

Start Time

Hour

15

Minute

0

?

Stop Time

Hour

18

Minute

0

OK

Cancel

Select **Create New > Schedule Group** and add create the schedule group by adding the outside of class time schedules to a schedule group.

New Schedule Group

Name

non-class time

Members

after class

X

+

before class

X

lunch

X

OK

Cancel

## 2. Creating a policy to block mobile devices outside of class time

Go to **Policy & Objects > Policy > IPv4** and create a policy that allows Internet access for mobile devices on the Student-net wireless network according to the schedule.

Set **Incoming Interface** to the wireless interface, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to the Internet-facing interface, and set **Schedule** to the new schedule group.

*Using a device group will automatically enable device identification on the wireless interface.*

New Policy

Incoming Interface

Ednet (SSID: Student-net)

+

Source Address

all

+

Source User(s)

Click to add...

Source Device Type

Mobile Devices

X

+

Outgoing Interface

port1

+

Destination Address

all

+

Schedule

non-class time

Service

ALL

+

Action

ACCEPT

Firewall / Network Options

ON

NAT

Use Outgoing Interface Address

Fixed Port

## 3. Results

Verify that mobile devices can connect to the Internet outside of class time, when the schedule group is valid.

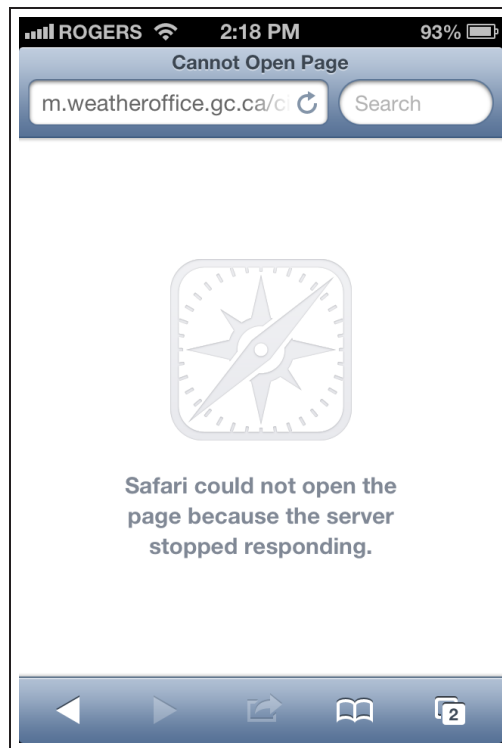
Go to **Log & Report > Traffic Log > Forward Traffic** to view mobile device traffic.

| #   | Date/Time | Src         | Device        | Dst            |
|-----|-----------|-------------|---------------|----------------|
| 161 | 17:00:48  | 20.10.10.40 | Android Phone | 8.8.8.8        |
| 162 | 15:00:28  | 20.10.10.40 | Android Phone | 216.250.166.65 |
| 163 | 12:58:38  | 20.10.10.40 | Android Phone | 65.55.172.252  |
| 164 | 12:48:26  | 20.10.10.41 | iPad          | 17.172.208.30  |
| 165 | 7:44:46   | 20.10.10.41 | iPad          | 8.8.8.8        |



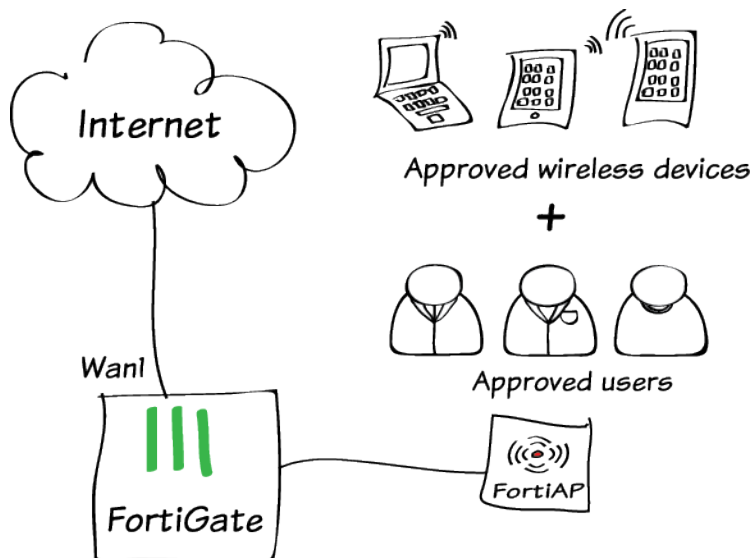
When the time in the schedule is reached, further surfing cannot continue.

This traffic does not appear in the logs, as only allowed traffic is logged.



For further reading, check out [Managing "bring your own device"](#) in the [FortiOS 5.2 Handbook](#).

# BYOD for a user with multiple wireless devices



In this example, you will make a FortiOS security policy that requires both user and device authentication, so that known users can only access the network when they are using known devices.

Using a combination of user and device authentication improves security in BYOD environments. Any authenticated user can connect through wireless, using any wireless device that is included in the device group specified in the policy. Thus, the BYOD policy can even support a user with multiple devices.

## 1. Create users and a user group

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.

The screenshot shows the 'Login Credentials' step of the user definition process. At the top, there are four steps: 'User Type' (checked), 'Login Credentials' (active), 'Contact Info', and 'Extra Info'. Below the steps, there are two input fields: 'User Name' with the value 'rgreen' and 'Password' with masked characters. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

The screenshot shows the 'User Groups' form. It has three sections: 'Name' with the value 'employees', 'Type' with radio buttons for 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest', and 'Members' with a list of users: 'gbrown' and 'rgreen'. Each user entry has a delete icon (X) and an add icon (+).

## 2. Create devices and a device group

Go to **User & Device > Device > Device Definitions** and enter the user's device information.

The screenshot shows the 'Device Definitions' form. It has several fields: 'Alias' with the value 'rgreen tablet', 'MAC Address' with the value '08:fd:0e:ff:0c:56', 'Additional MACs' with a dropdown menu showing 'Click to add...', 'Device Type' with a dropdown menu showing 'Android Tablet', 'Custom Groups' with a dropdown menu showing 'None', and 'Comments' with a text area. At the bottom right, there is a character count '0/255'.

Go to **User & Device > Device > Device Groups**. Create a device group and add user's devices to it.

The screenshot shows the 'Device Groups' form. It has three sections: 'Name' with the value 'staff devices', 'Members' with a list of devices: 'rgreen tablet'. Each device entry has a delete icon (X) and an add icon (+). At the bottom right, there is a character count '0/255'.

### 3. Configure WiFi security

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network for WPA-Enterprise authentication using the employees user group.

WiFi Settings

SSID

example-staff

Security Mode

WPA2 Enterprise

Authentication

☒ Local ☐ RADIUS Server

employees

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

Optional VLAN ID

0

### 4. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy to enable traffic from the WiFi interface to the Internet (in the example, *wan1*) and office LAN (in the example, *Internal*) interfaces.

Restrict the policy to allow only the employees user group and device group.

Incoming Interface

example-wifi (SSID: example-staff)

Source Address

example-wifi-net

Source User(s)

employees

Source Device Type

staff devices

Outgoing Interface

wan1

Internal

Destination Address

all

Schedule

always

Service

ALL

Action

✓ ACCEPT

## 5. Results

User **rgreen** can connect to the Internet using the **rgreen tablet** that belongs to the **staff devices** group.

| Policy ID | Source Interface/Zone | Destination Interface/Zone | Action | Active Sessions | Bytes    | Packets |
|-----------|-----------------------|----------------------------|--------|-----------------|----------|---------|
| 4         | example-wifi          | wan1, Internal             | ✓      | 30              | 79.12 MB | 124,095 |

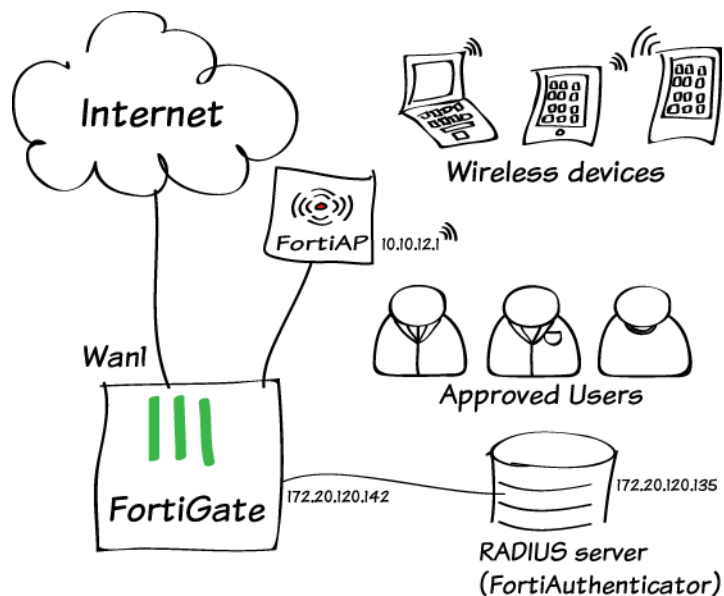
Go to **Policy & Objects > Monitor > Policy Monitor** to see the security policy in use.

Attempts to access the Internet fail if any of the following are true:

- the user does not belong to the employees user group
- the device does not belong to the staff devices group

For further reading, check out **Deploying Wireless Networks** in the **FortiOS 5.2 Handbook**.

# WiFi RADIUS authentication with FortiAuthenticator



In this example, you use an external RADIUS server to authenticate your WiFi clients.

In the example, a FortiAuthenticator (v3.00-build0176) is used as a RADIUS server to authenticate users who belong to the employees user group.

# 1. Create the user accounts and user group on the FortiAuthenticator

Go to **Authentication > User Management > Local Users** and create a user account.

**User Role** settings are available after you click **OK**.

Create additional user accounts as needed, one for each employee.

Go to **Authentication > User Management > User Groups** and create the local user group "employees" on the FortiAuthenticator.

Add users who are allowed to use the WiFi network.

The screenshot shows the 'Add User' form in FortiAuthenticator. The 'Username' field is set to 'rgreen'. The 'Disabled' checkbox is unchecked. 'Password-based authentication' is checked, with a '[Change Password]' link. 'Token-based authentication' and 'Enable account expiration' are unchecked. Under the 'User Role' section, the 'Role' is set to 'User' (selected with a radio button), while 'Administrator' is unselected. 'Allow RADIUS authentication' is checked, and 'Allow LDAP browsing' is unchecked.

The screenshot shows the 'Add User Group' form. The 'Name' field is 'employees'. The 'Type' is set to 'Local' (selected with a radio button), and 'Remote LDAP' is unselected. In the 'Users' section, there are two lists: 'Available users' and 'Selected users'. The 'Available users' list contains: admin, gbrown, hslimpson, jsmith, mburns, twhite, wloman. The 'Selected users' list contains: rgreen. At the bottom, there are buttons for 'Choose all visible' and 'Remove all'.

# 2. Register the FortiGate as a RADIUS client on the FortiAuthenticator

Go to **Authentication > RADIUS Service > Clients** and create a user account.

Enable all of the **EAP types**.

The screenshot shows the 'Add RADIUS Client' form. The 'Name' is 'FortiGate-1'. The 'Client name/IP' is '172.20.120.142'. The 'Secret' is masked with dots. The 'Description' is '200D'. Under 'Authentication method', 'Password-only authentication (exclude users without a password)' is selected. Under 'Username input format', 'username@realm' is selected. The 'Realms' section shows a table with one realm: 'local | Local users'. The 'Default' column is checked, and the 'Groups' column has a dropdown set to 'employees [edit]'. At the bottom, 'Allow MAC-based authentication' and 'Check machine authentication' are unchecked. Under 'EAP types', all four options are checked: EAP-GTC, EAP-TLS, PEAP, and EAP-TTLS.

| Default                             | Realm               | Allow local users to override remote users | Use Windows AD domain authentication | Groups  | Delete                   |
|-------------------------------------|---------------------|--|--------------------------------------|---|--------------------------|
| <input checked="" type="checkbox"/> | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | <input checked="" type="checkbox"/> Filter: employees [edit]<br><input type="checkbox"/> Filter local users: [edit] | <input type="checkbox"/> |

### 3. Configure FortiGate to use the RADIUS server

Go to **User & Device > Authentication > RADIUS Servers** and add the FortiAuthenticator unit as a RADIUS server.

|                             |  |                                     |
|-----------------------------|--|-------------------------------------|
| Name                        | <input type="text" value="facRADIUS"/>                                 |                                     |
| Primary Server IP/Name      | <input type="text" value="172.20.120.135"/>                            |                                     |
| Primary Server Secret       | <input type="password" value="••••••••"/>                              | <input type="button" value="Test"/> |
| Secondary Server IP/Name    | <input type="text"/>   |                                     |
| Secondary Server Secret     | <input type="password"/>   | <input type="button" value="Test"/> |
| Authentication Method       | <input checked="" type="radio"/> Default <input type="radio"/> Specify |                                     |
| NAS IP / Called Station ID  | <input type="text"/>   |                                     |
| Include in every User Group | <input type="checkbox"/>   |                                     |

### 4. Create the SSID and set up authentication

Go to **WiFi Controller > WiFi Network > SSID** and define your wireless network.

|                 |  |
|-----------------|--|
| Interface Name  | <input type="text" value="example-wifi"/>                  |
| Type            | <input type="text" value="WiFi SSID"/>                     |
| Traffic Mode    | <input type="text" value="Tunnel to Wireless Controller"/> |
| IP/Network Mask | <input type="text" value="10.10.12.1/255.255.255.0"/>      |

Set up DHCP for your clients.

| DHCP Server     | <input checked="" type="checkbox"/> Enable   |             |        |            |              |
|-----------------|--|-------------|--------|------------|--------------|
| Address Range   | <div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.12.2</td><td>10.10.12.100</td></tr></tbody></table></div> | Starting IP | End IP | 10.10.12.2 | 10.10.12.100 |
| Starting IP     | End IP   |             |        |            |              |
| 10.10.12.2      | 10.10.12.100   |             |        |            |              |
| Netmask         | <input type="text" value="255.255.255.0"/>   |             |        |            |              |
| Default Gateway | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |            |              |
| DNS Server      | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify   |             |        |            |              |

Configure WPA2 Enterprise security that uses the external RADIUS server.

|                          |  |
|--------------------------|--|
| WiFi Settings            |  |
| SSID                     | <input type="text" value="example-staff"/>                                 |
| Security Mode            | <input type="text" value="WPA2 Enterprise"/>                               |
| Authentication           | <input type="radio"/> Local <input checked="" type="radio"/> RADIUS Server |
|                          | <input type="text" value="facRADIUS"/>                                     |
| Broadcast SSID           | <input checked="" type="checkbox"/>  |
| Block Intra-SSID Traffic | <input checked="" type="checkbox"/>  |
| Maximum Clients          | <input type="checkbox"/>   |



# 5. Connect and authorize the FortiAP

Go to **System > Network > Interfaces** and configure a dedicated interface for the FortiAP.

Addressing mode

☐ Manual ☐ DHCP ☐ PPPoE ☒ Dedicated to Extension Device

IP/Network Mask

10.11.12.1/255.255.255.0

Connected Devices

None

Connect the FortiAP unit. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

|            |                  |        |               |                      |                        |                          |                  |                 |
|------------|------------------|--------|---------------|----------------------|------------------------|--------------------------|------------------|-----------------|
| Create New | Edit             | Delete | Refresh       | Display By           | AP                     | Radio                    | Managed FortiAPs | 1/64            |
| Mesh       | Access Point     | State  | Connected Via | SSIDs                | Channel                | Clients                  | OS Version       | FortiAP Profile |
|            | FP221C3X14019926 |        | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |                  | FAP221C-default |

When the FortiAP is listed, select and authorize it.

|            |                  |       |               |                      |                        |                          |            |                 |  |    |       |                  |      |
|------------|------------------|-------|---------------|----------------------|------------------------|--------------------------|------------|-----------------|--|----|-------|------------------|------|
| Create New |                  |       |               | Edit                 | Delete                 | Authorize                | Refresh    | Display By      |  | AP | Radio | Managed FortiAPs | 1/64 |
| Mesh       | Access Point     | State | Connected Via | SSIDs                | Channel                | Clients                  | OS Version | FortiAP Profile |  |    |       |                  |      |
| .          | FP221C3X14019926 |       | 10.11.12.2    | Radio 1:<br>Radio 2: | Radio1: 0<br>Radio2: 0 | Radio 1: 0<br>Radio 2: 0 |            | FAP221C-default |  |    |       |                  |      |

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.

Radio 2

Mode

☐ Disable ☒ Access Point

Spectrum Analysis

☐

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

5GHz 802.11ac/n/a

Select Channel Width

20MHz

Channel

☒ 36 ☐ 40 ☒ 44 ☐ 48 ☒ 149 ☐ 153 ☒ 157 ☐ 161 ☒ 165

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

example-wifi (SSID: exa...

## 5. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and add a policy that allows WiFi users to access the Internet.

|   |                                    |   |
|---|------------------------------------|---|
| Incoming Interface                      | example-wifi (SSID: example-staff) | + |
| Source Address                          | all                                | + |
| Source User(s)                          | Click to add...                    |   |
| Source Device Type                      | Click to add...                    |   |
| Outgoing Interface                      | wan1                               | + |
| Destination Address                     | all                                | + |
| Schedule                                | always                             |   |
| Service                                 | ALL                                | + |
| Action                                  | ACCEPT                             |   |
| <b>Firewall / Network Options</b>       |                                    |   |
| <input checked="" type="checkbox"/> NAT |                                    |   |

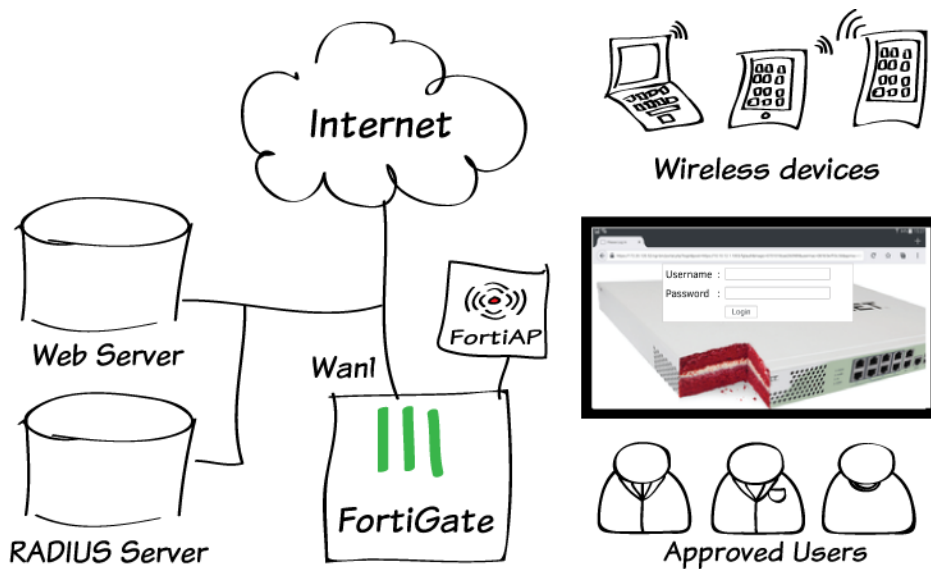
## Results

Go to **WiFi Controller > Monitor > Client Monitor** to see that clients connect and authenticate.

| SSID          | FortiAP              | User   | IP         | Device            | Channel | Bandwidth Tx/Rx |  |
|---------------|----------------------|--------|------------|-------------------|---------|-----------------|--|
| example-staff | FP221C3X14019926 (2) | rgreen | 10.10.12.2 | 08:fd:0e:ff:0c:56 | 165     | 10.18 Kbps      |  |

For further reading, check out the  
**Deploying Wireless Networks** in the  
FortiOS 5.2 Handbook.

# Using an external captive portal for WiFi security



In this example, wireless users are redirected to a captive portal web page (no matter what URL they enter) that requires them to authenticate before they can access the Internet. The portal page can also contain links to local information such as legal notices, terms of service and so on. This is sometimes called a “walled garden”.

The web portal page is a script that gathers the user’s logon credentials and sends back to the FortiGate a POST message of the format `https://<FGT_IP>:1000/fgtauth` with data `magic=session_id&username=<username>&password=<password>`. (The magic value was provided in the initial FortiGate request to the web server.) The script used for this example is [here](#).

A RADIUS server provides authentication.

# 1. Add the RADIUS server

Go to **User & Device > Authentication > RADIUS Servers**. Define the connection to the RADIUS server.

Name

fac\_radius

Primary Server IP/Name

172.20.120.135

Primary Server Secret

••••••••

Test Connectivity

Secondary Server IP/Name

Secondary Server Secret

Test Connectivity

Authentication Method

☒ Default ☐ Specify

NAS IP / Called Station ID

Include in every User Group

☐

Go to **User & Device > User > User Groups**. Define a firewall user group with the RADIUS server as its only member.

Name

extradius

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

Click to add...

Remote groups

Create New Edit Delete

| Remote Server | Group Name |
|---------------|------------|
| fac_radius    | Any        |

# 2. Enable HTTPS authentication

Use the CLI to enable use of HTTPS for authentication so that user credentials are communicated securely.

```
config user setting
set auth-secure-http enabled
end
```

# 3. Create the WiFi network

Go to **WiFi Controller > WiFi Network > SSID** to create the WiFi SSID.

Interface Name

example-wifi

Type

WiFi SSID

Traffic Mode

Tunnel to Wireless Controller

IP/Network Mask

10.10.12.1/255.255.255.0

Enable DHCP for clients.

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.10.12.2  | 10.10.12.100 |

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Same as Interface IP ☐ Specify

Configure external captive portal security.

Do not include "http://" or "https://" in the captive portal URL.

WiFi Settings

SSID

example-staff

Security Mode

Captive Portal

Portal Type

☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only

Authentication Portal

☐ Local ☒ External 172.20.120.52/cgi-bin/portal.php

User Groups

extradius

Exempt List

Click to add...

Redirect after Captive Portal

☒ Original Request ☐ Specific URL

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Split Tunneling

☐

Optional VLAN ID

0

#### 4. Create a "walled garden"

Go to **Policy & Objects > Objects > Addresses** and create an address for the captive portal.

Name

ecp

Type

IP/Netmask

Subnet / IP Range

172.20.120.52

Interface

wan1

Show in Address List

☒

Comments

0/255

Go to **Policy & Objects > Policy > IPv4**.  
Create a security policy for unauthenticated users that allows access only to the captive portal.

|                     |                                    |   |
|---------------------|------------------------------------|---|
| Incoming Interface  | example-wifi (SSID: example-staff) | + |
| Source Address      | all                                | + |
| Source User(s)      | Click to add...                    |   |
| Source Device Type  | Click to add...                    |   |
| Outgoing Interface  | wan1                               | + |
| Destination Address | ecp                                | + |
| Schedule            | always                             |   |
| Service             | ALL                                | + |
| Action              | ACCEPT                             |   |

**Firewall / Network Options**

ON

NAT

Use Outgoing Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

In the CLI, enable bypass of the captive portal so that the user can make the initial contact with the external server.

```
config firewall policy
```

endObtain <policy\_id> from ID column of the policy list (**Policy & Objects**)

**Policy > IPv4**).

### 5. Create the Internet access security policy

Go to **Policy & Objects > Policy > IPv4**.  
Create a policy to allow authenticated users access to the Internet.

|                     |                                    |     |
|---------------------|------------------------------------|-----|
| Incoming Interface  | example-wifi (SSID: example-staff) | +   |
| Source Address      | example-wifi-net                   | +   |
| Source User(s)      | extradius                          | X + |
| Source Device Type  | Click to add...                    |     |
| Outgoing Interface  | wan1                               | +   |
| Destination Address | all                                | +   |
| Schedule            | always                             |     |
| Service             | ALL                                | +   |
| Action              | ACCEPT                             |     |

**Firewall / Network Options**

ON

NAT

Use Outgoing Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

### 6. Connect and authorize the FortiAP

Go to **System > Network > Interface**.  
Edit an unused interface, making it

*Dedicated to Extension Device.* Connect the FortiAP to this interface and apply power. Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. Select and authorize the FortiAP.

Go to **WiFi Controller > WiFi Network > FortiAP Profiles**. Edit the default profile for your FortiAP model. Enable your SSID for each radio.

**Radio 1**

Mode ☐ Disable ☒ Access Point ☐ Dedicated Monitor

Spectrum Analysis ☐

WIDS Profile


Radio Resource Provision ☒


Client Load Balancing ☐ Frequency Handoff ☐ AP Handoff

Band

Channel ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Auto TX Power Control ☒ Disable ☐ Enable

TX Power 

SSID  

## Results

The WiFi network's security shows as Open. The device can associate and is assigned an IP address.

On the first attempt to browse the Internet, the captive portal screen is displayed.

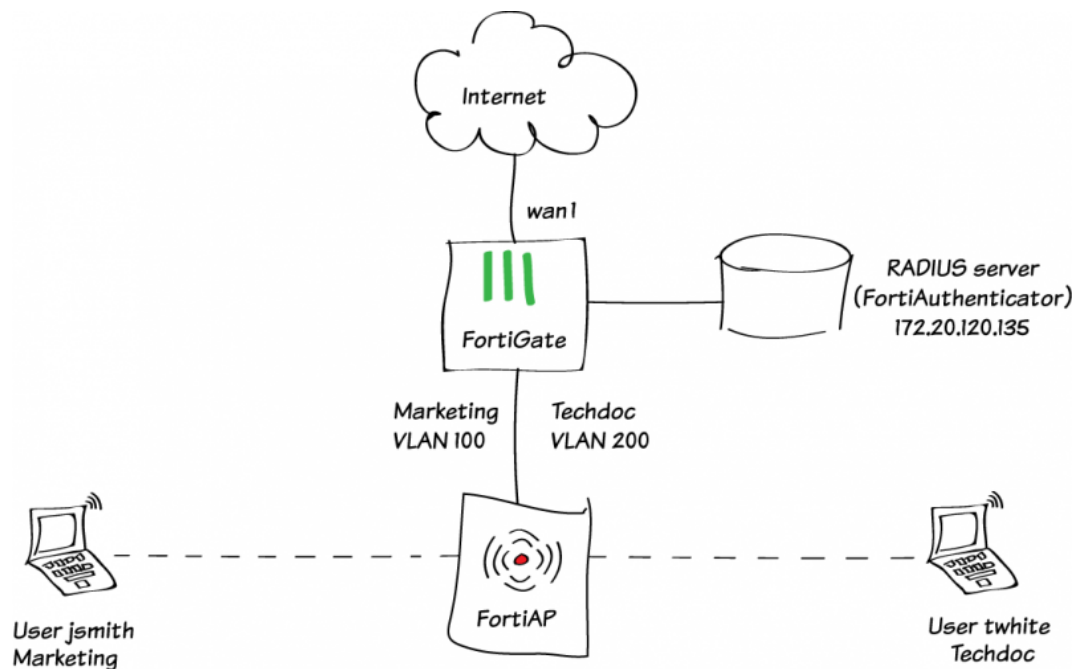
(The web server certificate must be verifiable, or the browser will show warnings.)

After authentication, the browser can access Internet destinations.





# Assigning WiFi users to VLANs dynamically



Virtual LANs (VLANs) are used to assign wireless users to different networks without requiring the use of multiple SSIDs. Each user's VLAN assignment is stored in the user database of the RADIUS server that authenticates the users.

This example creates dynamic VLANs for the Techdoc and Marketing departments. The RADIUS server is a FortiAuthenticator.

# 1. Configure the FortiAuthenticator

Go to **Authentication > RADIUS Service > Clients** to register the FortiGate as a client.

Enter a **Secret** (a password) and remember it. It will also be used in the FortiGate configuration.

Name:

FortGate-1

Client name/IP:

172.20.120.142

Secret:

\*\*\*\*\*

Description:

200D

Authentication method:

☐ Enforce two-factor authentication

☐ Apply two-factor authentication if available (authenticate any user)

☒ Password-only authentication (exclude users without a password)

☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm

☐ realmusername

☐ realm/username

Realms:

| Default                          | Realm               | Allow local users to override remote users | Use Windows AD domain authentication | Groups   | Delete |
|----------------------------------|---------------------|--|--------------------------------------|--|--------|
| <input checked="" type="radio"/> | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | <div><input checked="" type="checkbox"/> Filter: employees [Edit]<br/><input type="checkbox"/> Filter: local users: [Edit]</div> |        |

Add a realm

☐ Allow MAC-based authentication

☐ Check machine authentication

EAP types:

☒ EAP-GTC

☒ EAP-TLS

☒ PEAP

☒ EAP-TTLS

Go to **Authentication > User Management > Local Users** and create local user accounts as needed.

Username:

jsmith

☐ Disabled

☒ Password-based authentication

[Change Password]

☐ Token-based authentication

☒ Allow RADIUS authentication

☐ Enable account expiration

User Role

Role:

☐ Administrator

☒ User

☐ Allow LDAP browsing

For each user, add these RADIUS

attributes which specify the VLAN information to be sent to the FortiGate. Tunnel-Private-Group-Id specifies the VLAN ID.

In this example, jsmith is assigned VLAN 100 and twwhite is assigned VLAN 200.

## 2. Add the RADIUS server to the FortiGate configuration

Go to **User & Device > Authentication > RADIUS Servers**. Select **Create New**.

Enter the FortiAuthenticator IP address and the server secret that you entered on the FortiAuthenticator.

Optionally, you can click **Test Connectivity**. Enter a RADIUS user's ID and password. The result should be "Successful".

|                             |  |                                    |
|-----------------------------|--|------------------------------------|
| Name                        | fac_radius   |                                    |
| Primary Server IP/Name      | 172.20.120.135   |                                    |
| Primary Server Secret       | *****  | <button>Test Connectivity</button> |
| Secondary Server IP/Name    |  |                                    |
| Secondary Server Secret     |  | <button>Test Connectivity</button> |
| Authentication Method       | <input checked="" type="radio"/> Default <input type="radio"/> Specify |                                    |
| NAS IP / Called Station ID  |  |                                    |
| Include in every User Group | <input type="checkbox"/>   |                                    |

## 3. Create an SSID with dynamic VLAN assignment

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID and set up DHCP service.

| Interface Name        | Dynamic_VLAN   |             |        |            |              |
|-----------------------|--|-------------|--------|------------|--------------|
| Type                  | WiFi SSID  |             |        |            |              |
| Traffic Mode          | Tunnel to Wireless Controller  |             |        |            |              |
| IP/Network Mask       | 10.11.12.1/255.255.255.0   |             |        |            |              |
| Administrative Access | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access |             |        |            |              |
| DHCP Server           | <input checked="" type="checkbox"/> Enable   |             |        |            |              |
| Address Range         | <div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.11.12.2</td><td>10.11.12.254</td></tr></tbody></table></div>   | Starting IP | End IP | 10.11.12.2 | 10.11.12.254 |
| Starting IP           | End IP   |             |        |            |              |
| 10.11.12.2            | 10.11.12.254   |             |        |            |              |
| Netmask               | 255.255.255.0  |             |        |            |              |
| Default Gateway       | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |            |              |
| DNS Server            | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify   |             |        |            |              |

Select WPA2 Enterprise security and select your RADIUS server for authentication.

Set the default VLAN ID to 10. This VLAN is used when RADIUS doesn't assign a VLAN.

WiFi Settings

SSID

Dynamic\_VLAN\_SSID

Security Mode

WPA2 Enterprise

Authentication

Local

RADIUS Server

fac\_radius

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Split Tunneling

☐

Optional VLAN ID

10

Go to **System > Dashboard > Status** and use the **CLI Console** to enable dynamic VLANs on the SSID.

```
config wireless-controller vap
edit Dynamic_VLAN
set dynamic-vlan enable
end
```

## 4. Create the VLAN interfaces

Go to **System > Network > Interfaces**.

Create the VLAN interface for default VLAN-10 and set up DHCP service.

Interface Name

VLAN-10

Type

VLAN

Interface

Dynamic\_VLAN (SSID: Dy

VLAN ID

10

Addressing mode

Manual

DHCP

PPPoE

IP/Network Mask

192.168.2.1/255.255.255.0

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

☐ FCT-Access

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP        |
|-------------|---------------|
| 192.168.2.2 | 192.168.2.254 |

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

Create the VLAN interface for marketing-100 and set up DHCP service.

Interface Name

marketing-100

Type

VLAN

Interface

Dynamic\_VLAN (SSID: for

VLAN ID

100

Addressing mode

Manual

DHCP

PPPoE

IP/Network Mask

10.11.13.1/24

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

☐ FCT-Access

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.11.13.2  | 10.11.13.254 |

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

Create the VLAN interface for techdoc-200 and set up DHCP service.

Interface Name

techdoc-200

Type

VLAN

Interface

Dynamic\_VLAN (SSID: for

VLAN ID

200

Addressing mode

Manual

DHCP

PPPoE

IP/Network Mask

10.11.14.1/24

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

☐ FCT-Access

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

| Starting IP | End IP       |
|-------------|--------------|
| 10.11.14.2  | 10.11.14.254 |

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

## 5. Create security policies

Go to **Policy > Policy > IPv4**.

Create a policy that allows outbound traffic from marketing-100 to the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | marketing-100   | + |
| Source Address      | all             | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | wan1            | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

In **Logging Options**, enable logging for all sessions.

**Logging Options**

☒ Log Allowed Traffic

☐ Security Events

☒ All Sessions

Create a policy that allows outbound traffic from techdoc-200 to the Internet.

For this policy too, in **Logging Options** enable logging for all sessions.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | techdoc-200     | + |
| Source Address      | all             | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | wan1            | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 6. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles**.

Create a new profile for your FortiAP model and select the new SSID for both Radio 1 and Radio 2.

The screenshot shows the configuration page for a FortiAP profile named 'FAP221C-dyn-vlan'. The 'Name' field is filled with 'FAP221C-dyn-vlan', 'Comments' is empty, 'Platform' is 'FAP221C', and 'Split Tunneling Subnets(s)' is empty. Under the 'Radio 1' section, 'Mode' is set to 'Access Point', 'Spectrum Analysis' is unchecked, 'WIDS Profile' is 'default', 'Radio Resource Provision' is checked, 'Client Load Balancing' is unchecked, 'Band' is '2.4GHz 802.11n/g/b', 'Channel' is '1', 'Auto TX Power Control' is 'Disable', and 'TX Power' is set to 100%. The 'SSID' field is 'Dynamic\_VLAN (SSID: ...)'.

## 7. Connect and authorize the FortiAP

Go to **System > Network > Interfaces** and choose an unused interface. Set **Addressing mode** to **Dedicated to Extension Device**. Connect the FortiAP unit to the this interface and apply power.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**.

Right-click on the FortiAP unit and select the FortiAP profile that you created. Right-click on the FortiAP unit again. Select **Authorize**.

The screenshot shows the 'Managed FortiAPs' table. A context menu is open over the first row, which has 'Access Point' mode, 'State' 'Authorized', 'Connected Via' '192.168.1.3', and 'SSIDs' 'Radio 1: (Disabled), Radio 2: (Disabled)'. The 'Assign Profile' option is selected, showing a submenu with 'FAP221C-default', 'FAP221C-dyn-vlan' (checked), and 'FAP221C-mesh'.

| Mesh | Access Point     | State      | Connected Via | SSIDs                                      | Channel | Clients | Version |
|------|------------------|------------|---------------|--|---------|---------|---------|
| -    | FP221C3X14019926 | Authorized | 192.168.1.3   | Radio 1: (Disabled)<br>Radio 2: (Disabled) |         |         | v5.2    |

# Results

















The SSID will appear in the list of available wireless networks on the users' devices. Both twhite and jsmith can connect to the SSID with their credentials and access the Internet.

(If a certificate warning message appears, accept the certificate.)

Go to **Log & Report > Traffic Log > Forward Traffic Log**.

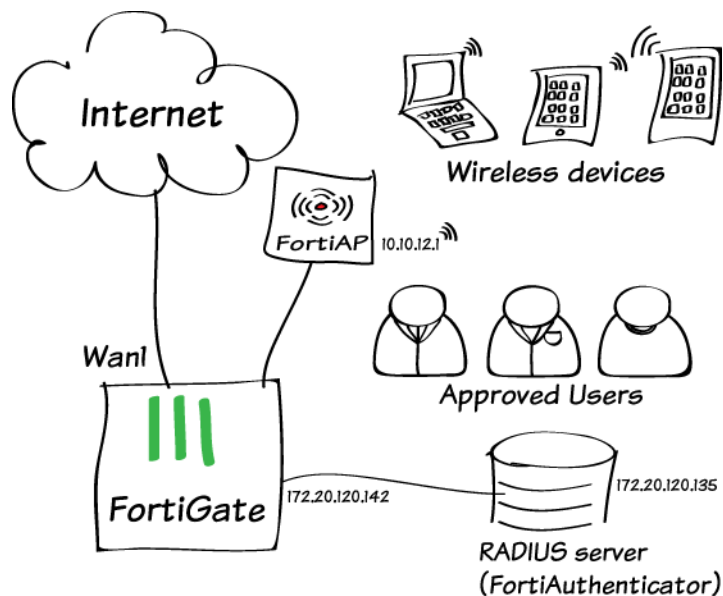
Note that traffic for jsmith and twhite pass through different policies. The policy IDs correspond to the marketing-100 and techdoc-200 policies respectively.

The security policies could be made different so that Marketing and Techdoc departments are allowed different access, but we didn't think that was fair.

| Date/Time | Source  | Destination  | Action | Policy ID |
|-----------|---|--|--------|-----------|
| 12:42:06  |  jsmith (10.11.13.2) |  63.140.35.161 (metrics.cbc.ca)               | close  | 7         |
| 12:42:06  |  jsmith (10.11.13.2) |  63.140.35.161 (metrics.cbc.ca)               | close  | 7         |
| 12:41:52  |  jsmith (10.11.13.2) |  174.129.209.146 (api.samsungosp.com)         | close  | 7         |
| 12:41:48  |  jsmith (10.11.13.2) |  64.210.203.208 (bcmls2.glpals.com)           | close  | 7         |
| 12:40:59  |  twhite (10.11.14.2) |  208.80.52.126 (2073.live.streamtheworld.com) | close  | 9         |
| 12:40:53  |  twhite (10.11.14.2) |  209.114.50.168 (rc1.nobexinc.com)            | close  | 9         |
| 12:40:50  |  twhite (10.11.14.2) |  216.58.216.234 (play.googleapis.com)         | close  | 9         |
| 12:40:49  |  twhite (10.11.14.2) |  174.35.52.179 (api.accuweather.com)          | close  | 9         |



# WiFi with Wireless Single Sign-on



This is an example of wireless single-sign-on (WSSO) with a Fortigate. The WiFi users are teachers and students at a school. Each user belongs to a user group, either TeacherGroup or StudentGroup. A FortiAuthenticator performs user authentication and passes the user group name to the FortiGate so that the appropriate security policy is applied. The student security policy applies a more restrictive web filter.

# 1. Register the FortiGate as a RADIUS client on the FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and create an account. Enter and remember the **Secret** (password).

Enable all of the EAP types.

Name:

FortGate-1

Client name/IP:

172.20.120.142

Secret:

\*\*\*\*\*

Description:

200D

Authentication method:

☐ Enforce two-factor authentication

☐ Apply two-factor authentication if available (authenticate any user)

☒ Password-only authentication (exclude users without a password)

☐ FortiToken-only authentication (exclude users without a FortiToken)

Username input format:

☒ username@realm

☐ realmusername

☐ realm/username

Realms:

| Default                          | Realm               | Allow local users to override remote users | Use Windows AD domain authentication | Groups   | Delete |
|----------------------------------|---------------------|--|--------------------------------------|--|--------|
| <input checked="" type="radio"/> | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | <div><input type="checkbox"/> Filter: employees [Edit]</div> <div><input type="checkbox"/> Filter: local users: [Edit]</div> |        |

  |

Add a realm

☐ Allow MAC-based authentication

☐ Check machine authentication

EAP types:

☒ EAP-GTC

☒ EAP-TLS

☒ PEAP

☒ EAP-TTLS

## 2. Create user accounts on the FortiAuthenticator

Go to **Authentication > User Management > Local Users** and create a user account.

**User Role** settings are available after you click OK.

The screenshot shows the 'Local Users' configuration page. At the top, the 'Username' field is set to 'jsmith'. Below this, there are several checkboxes: 'Disabled' (unchecked), 'Password-based authentication' (checked, with a '[Change Password]' link), 'Token-based authentication' (unchecked), 'Allow RADIUS authentication' (checked), and 'Enable account expiration' (unchecked). A section titled 'User Role' contains a 'Role:' label with two radio buttons: 'Administrator' (unchecked) and 'User' (checked). At the bottom, there is a checkbox for 'Allow LDAP browsing' which is unchecked.

## 3. Create user groups on the FortiAuthenticator

Go to **Authentication > User Management > User Groups**.

Create and populate TeacherGroup and StudentGroup.

The screenshot shows the 'User Groups' configuration page. The 'Name' field is set to 'TeacherGroup'. The 'Type' section has three radio buttons: 'Local' (selected), 'Remote LDAP' (unchecked), and 'Remote RADIUS' (unchecked). Below this, the 'Users' section contains two lists. The 'Available users' list on the left includes: gbrown, guest, hsimpson, jgarick, jsmith, nradd, rgreen, and twitter:wwilsonFortinet. The 'Selected users' list on the right includes: twhite and ckent. At the bottom, there are two buttons: 'Choose all visible' and 'Remove all'.

Re-edit each group. Add the Fortinet-Group-Name RADIUS attribute which specifies the user group name to be sent to the FortiGate.

Vendor: Fortinet  
Attribute ID: Fortinet-Group-Name  
Value: TeacherGroup or StudentGroup, as appropriate.

Create New User Group RADIUS Attribute

Vendor:

Fortinet

Attribute ID:

Fortinet-Group-Name

Type:

String

Value:

TeacherGroup

OK

Cancel

## 4. Configure FortiGate to use the RADIUS server

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers**. Select **Create New**.

Enter the FortiAuthenticator IP address and the server secret that you entered on the FortiAuthenticator.

Optionally, you can click **Test Connectivity**. Enter a RADIUS user's ID and password. The result should be "Successful".

Name

fac\_radius

Primary Server IP/Name

172.20.120.135

Primary Server Secret

••••••

Test Connectivity

Secondary Server IP/Name

Secondary Server Secret

Test Connectivity

Authentication Method

☒ Default ☐ Specify

NAS IP / Called Station ID

Include in every User Group

☐

## 5. Configure user groups on the FortiGate

Go to **User & Device > User > User Groups**. Create TeacherGroup and StudentGroup. Don't add any members.

Name

TeacherGroup

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

Click to add...

Remote groups

Create New

Edit

Delete

Remote Server

Group Name

No matching entries found

## 6. Create security policies

Go to **Policy & Objects > Policy > IPv4**. Create two WiFi-to-Internet policies. One has StudentGroup as the **Source User (s)**, the other specifies TeacherGroup. The student policy selects a more restrictive Web Filter.

|                     |                                    |     |
|---------------------|------------------------------------|-----|
| Incoming Interface  | example-wifi (SSID: example-staff) | +   |
| Source Address      | example-wifi-net                   | +   |
| Source User(s)      | StudentGroup                       | X + |
| Source Device Type  | Click to add...                    |     |
| Outgoing Interface  | wan1                               | +   |
| Destination Address | all                                | +   |
| Schedule            | always                             |     |
| Service             | ALL                                | +   |
| Action              | ACCEPT                             |     |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

**Security Profiles**

☒ ON AntiVirus default

☒ ON Web Filter students

☒ ON Application Control default

## 7. Create an SSID with RADIUS authentication

Go to **WiFi Controller > WiFi Network > SSID**. Create an SSID and set up DHCP for clients.

| Interface Name              | example-wifi   |             |        |            |              |
|-----------------------------|--|-------------|--------|------------|--------------|
| Type                        | WiFi SSID  |             |        |            |              |
| Traffic Mode                | Tunnel to Wireless Controller  |             |        |            |              |
| IP/Network Mask             | 10.10.12.1/255.255.255.0   |             |        |            |              |
| Administrative Access       | <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access<br><input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access |             |        |            |              |
| DHCP Server                 | <input checked="" type="checkbox"/> Enable   |             |        |            |              |
| Address Range               | <div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.12.2</td><td>10.10.12.100</td></tr></tbody></table></div>   | Starting IP | End IP | 10.10.12.2 | 10.10.12.100 |
| Starting IP                 | End IP   |             |        |            |              |
| 10.10.12.2                  | 10.10.12.100   |             |        |            |              |
| Netmask                     | 255.255.255.0  |             |        |            |              |
| Default Gateway             | <input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify  |             |        |            |              |
| DNS Server                  | <input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify   |             |        |            |              |
| <a href="#">Advanced...</a> |  |             |        |            |              |

Configure WPA2-Enterprise authentication that uses the FortiAuthenticator as RADIUS server.

WiFi Settings

SSID

example-staff

Security Mode

WPA2 Enterprise

Authentication

☐ Local

☒ RADIUS Server

fac\_radius

Broadcast SSID

☒

Block Intra-SSID Traffic

☒

Maximum Clients

☐

Split Tunneling

☐

Optional VLAN ID

0

## 8. Add the FortiAP

Go to **System > Network > Interface**. Dedicate an unused network interface to FortiAP.

Addressing mode

☐ Manual

☐ DHCP

☐ PPPoE

☒ Dedicated to Extension Device

IP/Network Mask

192.168.1.1/255.255.255.0

Connected Devices

None

Connect the FortiAP to the dedicated interface. Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. Wait the the FortiAP to be listed (refresh as needed). Select and **Authorize** the FortiAP.

| Display By: <input checked="" type="radio"/> AP <input type="radio"/> Radio |                  |       |               |                                 |                     |                       |            |                 |  |
|---|------------------|-------|---------------|---------------------------------|---------------------|-----------------------|------------|-----------------|--|
| Managed FortiAPs 1/64   |                  |       |               |                                 |                     |                       |            |                 |  |
| Mes   | Access Point     | State | Connected Via | SSIDs                           | Channel             | Clients               | OS Version | FortiAP Profile |  |
|   | FP221C3X14019926 |       | 192.168.1.3   | Radio 1: Radio 2: example-staff | Radio1: 0 Radio2: 0 | Radio 1: 0 Radio 2: 0 |            | FAP221C-default |  |

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and open the profile for your FortiAP model. Add your SSID to both radios.

Radio 1

Mode

☐ Disable

☒ Access Point

☐ Dedicated Monitor

Spectrum Analysis

☐

WIDS Profile

default

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff

☐ AP Handoff

Band

2.4GHz 802.11n/g/b

Channel

☒ 1

☐ 2

☐ 3

☐ 4

☐ 5

☒ 6

☐ 7

☐ 8

☐ 9

☐ 10

☒ 11

Auto TX Power Control

☒ Disable

☐ Enable

TX Power

100 %

SSID

example-wifi (SSID: exa...

# Results

Connect to the WiFi network, authenticate, and browse the Internet. Try this with both student and teacher accounts.

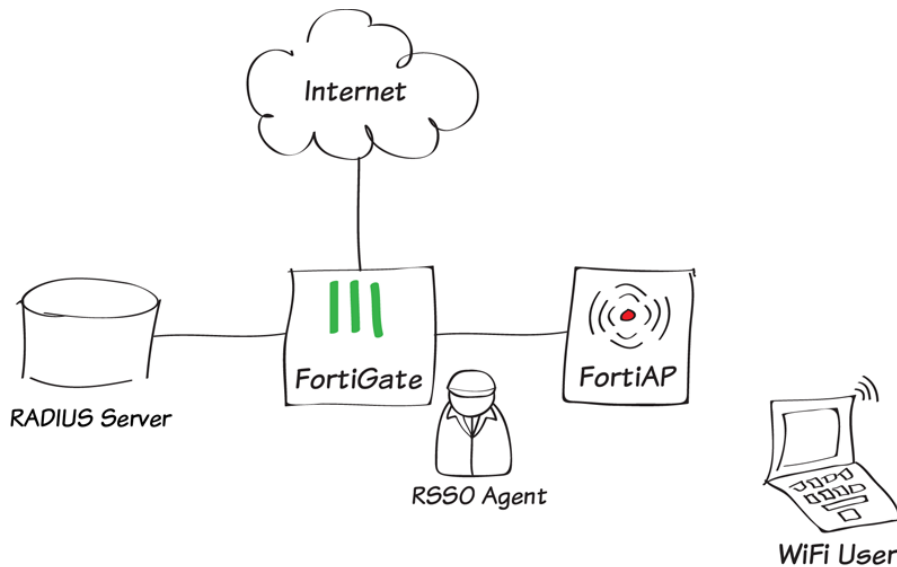
Go to **User & Device > Monitor > Firewall**. You can verify the User Group and that the WSSO authentication method was used.

| User Name | User Group   | IP Address | Method |  |
|-----------|--------------|------------|--------|--|
| gbrown    | StudentGroup | 10.10.12.2 | WSSO   |  |

Go to **Policy & Objects > Monitor > Policy Monitor**. You can verify that the appropriate security policy was applied.

| Policy ID | Source Interface/Zone | Destination Interface/Zone | Action | Active Sessions | Bytes   | Packets |
|-----------|-----------------------|----------------------------|--------|-----------------|---------|---------|
| 8         | example-wifi          | wan1                       |        | 7               | 1.04 GB | 966,789 |

# RSSO WiFi access control



In this example, you will use RADIUS Single Sign-On (RSSO) to authenticate wireless users.

Users will be required to enter their credentials, which are stored on a RADIUS server, when connecting to the wireless network. Once they have been authenticated, the same credentials will also be used by the FortiGate to allow outbound traffic without requiring additional authentication.

In this example, a FortiAP has already been installed in Tunnel mode. For more information, see [Setting up WiFi with FortiAP](#).



## 1. Adding a RADIUS server and allowing accounting messages to be accepted

Go to **User & Device > Authentication > RADIUS servers** and create a new server connection.

Set the **Primary Server IP/Name** and **Primary Server Secret**. Test the connection.

Configure additional settings as required.

Go to **System > Network > Interfaces** and edit the interface that communicates with the RADIUS server.

Enable **Listen for RADIUS Accounting Messages**.

|                                     |   |
|-------------------------------------|---|
| Name                                | <input type="text" value="RSSO_Server"/>    |
| Primary Server IP/Name              | <input type="text" value="172.20.120.135"/> |
| Primary Server Secret               | <input type="password" value="....."/>      |
| <input type="button" value="Test"/> |   |

|                                       |                                     |
|---------------------------------------|-------------------------------------|
| Enable Explicit Web Proxy             | <input type="checkbox"/>            |
| Listen for RADIUS Accounting Messages | <input checked="" type="checkbox"/> |
| Secondary IP Address                  | <input type="checkbox"/>            |

## 2. Creating an RSSO agent

Go to **User & Device > Authentication > Single Sign-On** and create a new agent.

Set **Type** to **RADIUS Single Sign-On Agent** and enable both **Use RADIUS Shared Secret** and **Send RADIUS Responses**.

|  |   |
|--|---|
| Type   | <input type="radio"/> Poll Active Directory Server <input type="radio"/> Fortinet Single-Sign-On Agent <input checked="" type="radio"/> RADIUS Single-Sign-On Agent |
| Name   | <input type="text" value="RSSO Agent"/>   |
| <input checked="" type="checkbox"/> Use RADIUS Shared Secret |   |
| Shared Secret  | <input type="password" value="....."/>  |
| <input checked="" type="checkbox"/> Send RADIUS Responses    |   |

## 3. Creating an RSSO user group

Go to **User & Device > User > User Groups** and create a new user group.

Set **Type** to **RADIUS Single Sign-On (RSSO)** and enter the **RADIUS Attribute Value**.

|                        |   |
|------------------------|---|
| Name                   | <input type="text" value="RSSO_group"/>   |
| Type                   | <input type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input checked="" type="radio"/> RADIUS Single Sign-On (RSSO) |
| RADIUS Attribute Value | <input type="text" value="tac"/> <input data-bbox="1121 1342 1144 1368" type="button" value="?"/>   |

## 4. Creating a security policy for the RSSO user group

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the wireless interface, **Source User(s)** to the RSSO user group, and **Outgoing Interface** to your Internet-facing interface.

The screenshot shows the 'Policy' configuration window for IPv4. The 'Incoming Interface' is set to 'WiFi (SSID: fortinet)'. The 'Source Address' is set to 'all'. The 'Source User(s)' is set to 'RSSO\_group'. The 'Source Device Type' is set to 'Click to add...'. The 'Outgoing Interface' is set to 'wan1'. The 'Destination Address' is set to 'all'. The 'Schedule' is set to 'always'. The 'Service' is set to 'ALL'. The 'Action' is set to 'ACCEPT'. Below the main configuration, the 'Firewall / Network Options' section is visible, with 'NAT' turned on. Under 'NAT', 'Use Outgoing Interface Address' is selected, and 'Fixed Port' is unchecked. There is also an option for 'Use Dynamic IP Pool' and a 'Click to add...' button.

## 5. Configuring the RADIUS server

In this example, a Microsoft Network Policy Server (NPS) is used as the RADIUS server.

Create a remote RADIUS server group.  
Set the IP address as the FortiGate unit's IP.

The screenshot shows the 'Remote RADIUS Server Groups' configuration window. The 'Group name' is set to 'Fortinet'. Below the group name, there is a table with columns 'RADIUS Server', 'Priority', and 'Weight'. The table contains one entry: '192.168.1.1' with a 'Priority' of '1' and a 'Weight' of '50'. At the bottom of the window, there are buttons for 'Add...', 'Edit...', 'Remove', 'OK', 'Cancel', and 'Apply'.

Go to **Authentication/Accounting**.

Deselect **Use the same share secret for authentication and accounting** and enter the same **secret** that is used by the RSO agent.

The screenshot shows the 'Edit RADIUS Server' dialog box with the 'Authentication/Accounting' tab selected. The 'Address' tab is also visible. The 'Authentication' section has the 'Authentication port' set to 1812, the 'Shared secret' and 'Confirm shared secret' fields are empty, and the 'Request must contain the message authenticator attribute' checkbox is unchecked. The 'Accounting' section has the 'Accounting port' set to 1813, the 'Use the same shared secret for authentication and accounting' checkbox is unchecked, and the 'Forward network access server start and stop notifications to this server' checkbox is checked. The 'Shared secret' and 'Confirm shared secret' fields are also empty in the accounting section. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

**Edit RADIUS Server**

Address Authentication/Accounting Load Balancing

Authentication port: 1812

Select an existing Shared Secrets template: None

Shared secret:

Confirm shared secret:

☐ Request must contain the message authenticator attribute

Accounting

Accounting port: 1813

☐ Use the same shared secret for authentication and accounting.

Select an existing Shared Secrets template: None

Shared secret:

Confirm shared secret:

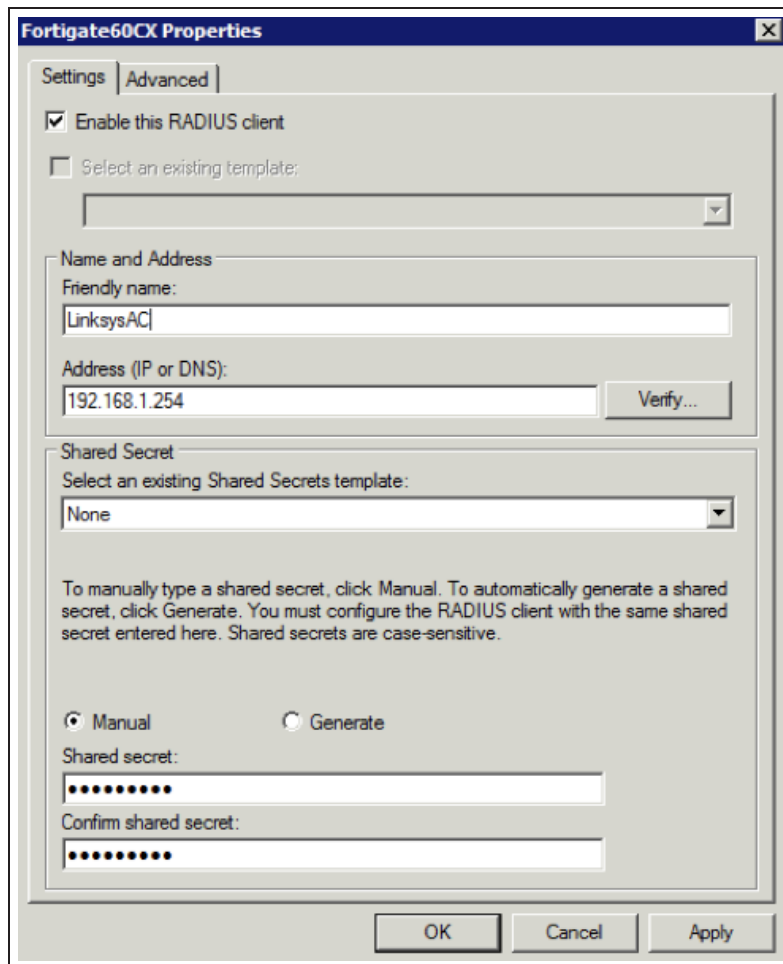
☒ Forward network access server start and stop notifications to this server

OK Cancel Apply

## 6. Configuring the RADIUS client

Create a new RADIUS client and go to **Properties**.

Select **Enable this RADIUS client**. Set **Name and Address** to match the FortiAP and enter the **Shared secret**.



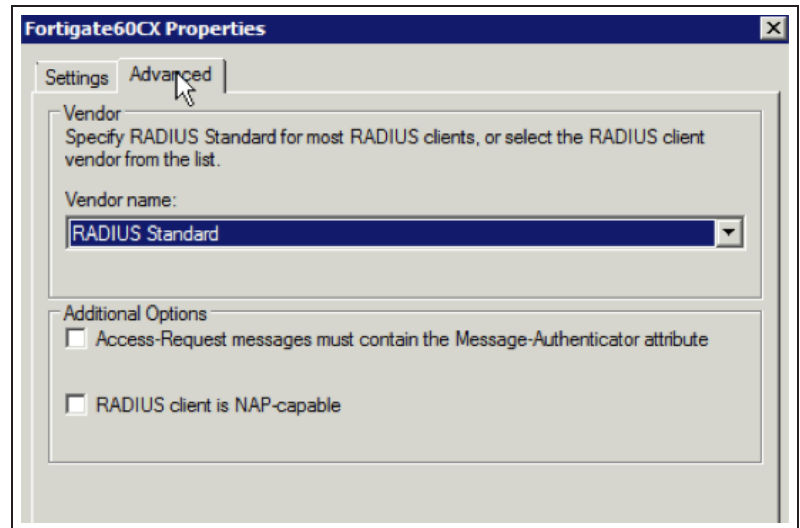
The image shows the 'Fortigate60CX Properties' dialog box with the 'Advanced' tab selected. The 'Settings' tab is also visible. The 'Advanced' tab contains the following fields and options:

- ☒ **Enable this RADIUS client**
- ☐ **Select an existing template:** (dropdown menu)
- Name and Address**
  - Friendly name:** LinksysAC
  - Address (IP or DNS):** 192.168.1.254 (with a 'Verify...' button)
- Shared Secret**
  - Select an existing Shared Secrets template:** None (dropdown menu)
  - Text: To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
  - ☒ **Manual** ☐ **Generate**
  - Shared secret:** (password field with 8 dots)
  - Confirm shared secret:** (password field with 8 dots)

At the bottom are buttons for **OK**, **Cancel**, and **Apply**.

Go to the **Advanced** properties.

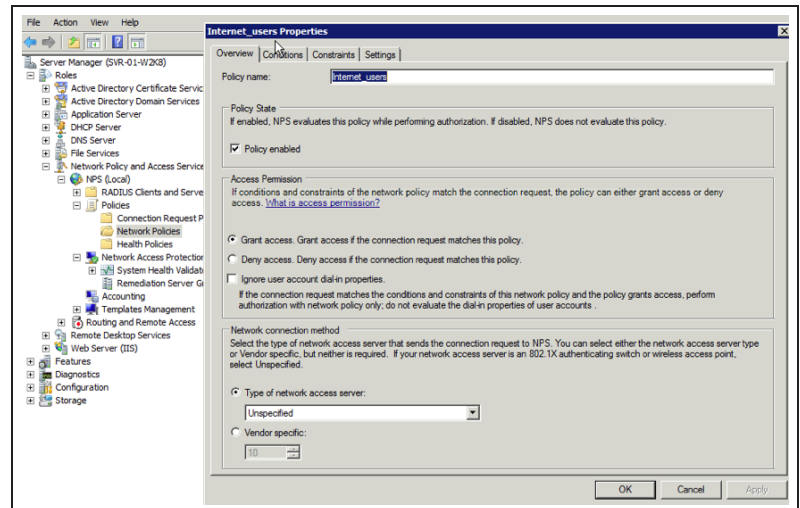
Set **Vendor name** to **RADIUS Standard**.



## 7. Creating a network policy

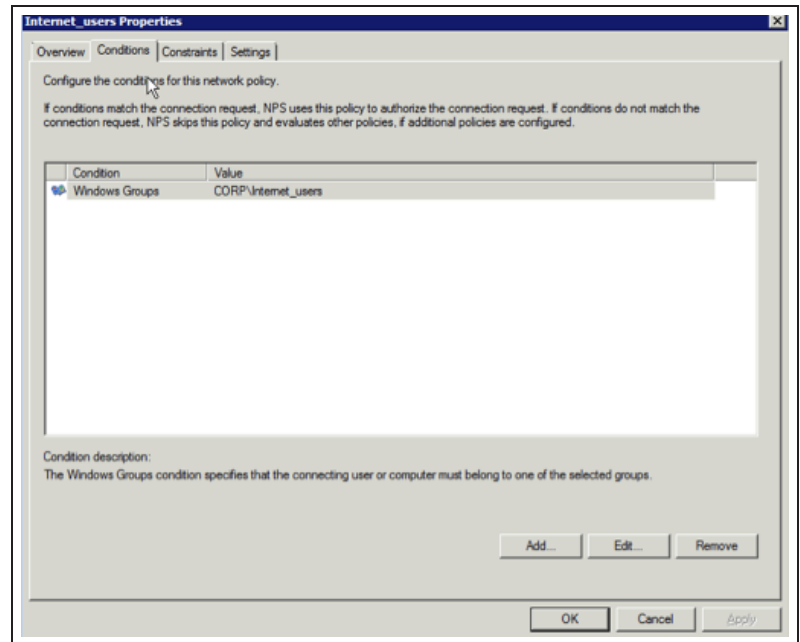
Create a new network policy.

Select **Policy enabled** and **Grant access**.



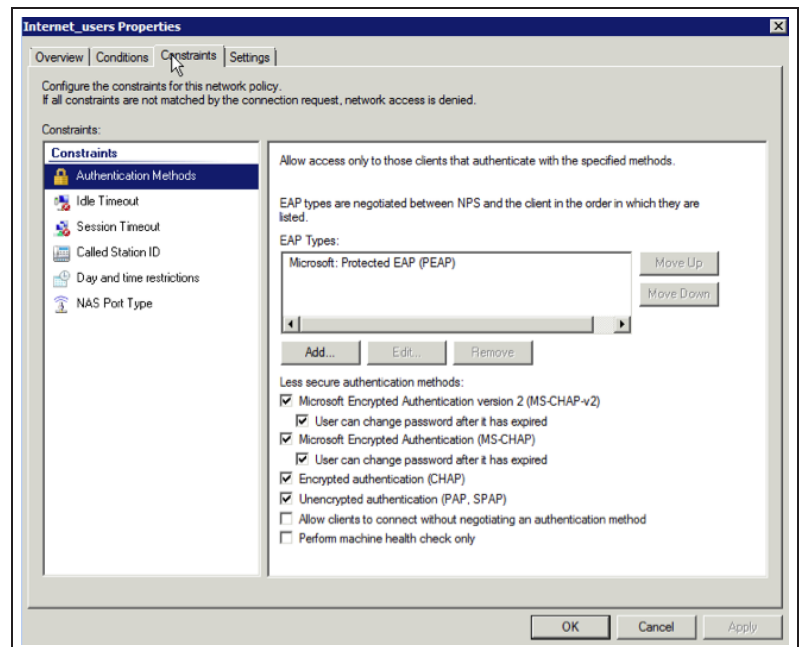
Go to **Conditions**.

Add **Windows Group** and select **Corp/Internet\_user** from the AD.



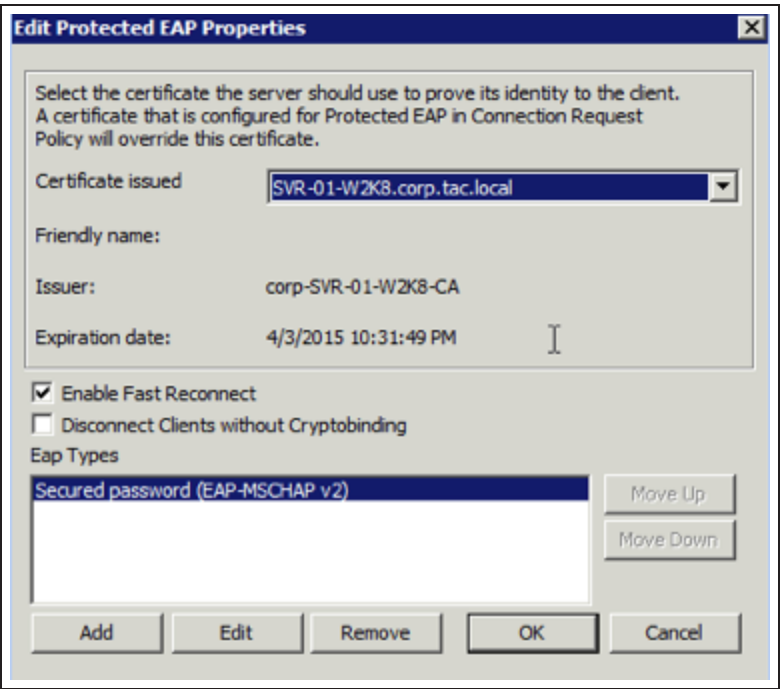
Go to **Constraints**.

Select **Authentication Methods** and add **Microsoft: Protected EAP (PEAP)** under **EAP Types**.



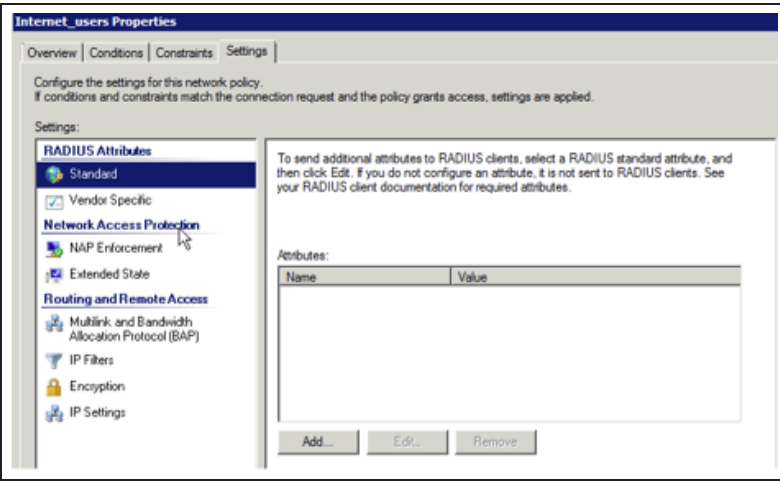
Select **PEAP** from the **EAP Types** list and select **Edit**.

Ensure that a certificate is issued for PEAP.



Go to **Settings**.

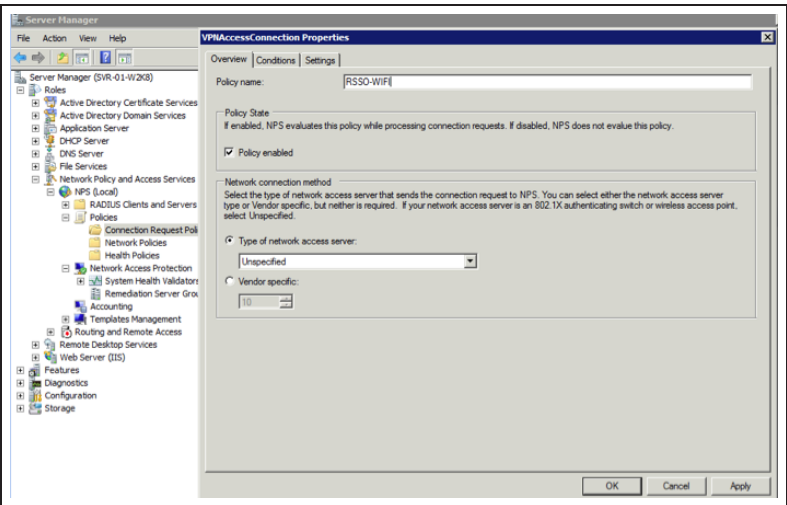
Select **Standard** and remove all attributes that are listed.



## 8. Creating a connection request policy

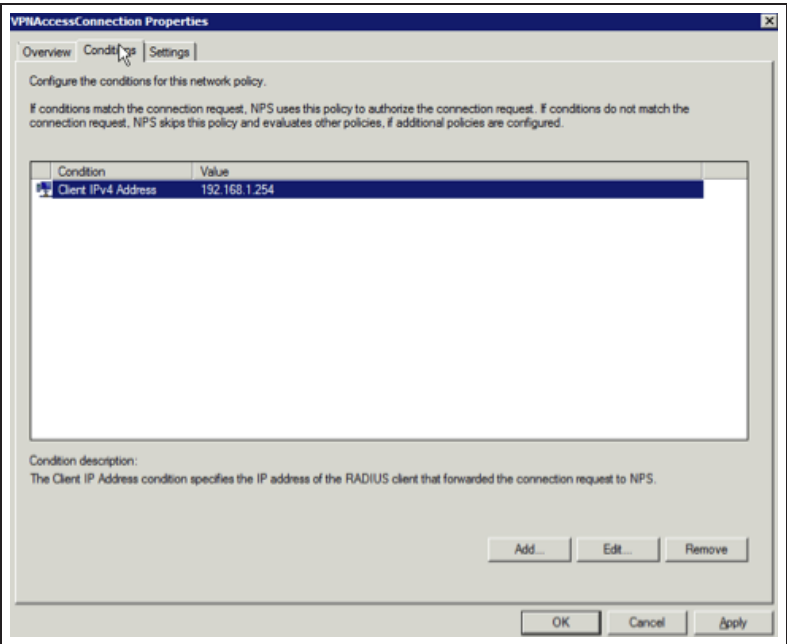
Create a new connection request policy.

Select **Policy enabled**.



Go to **Conditions**.

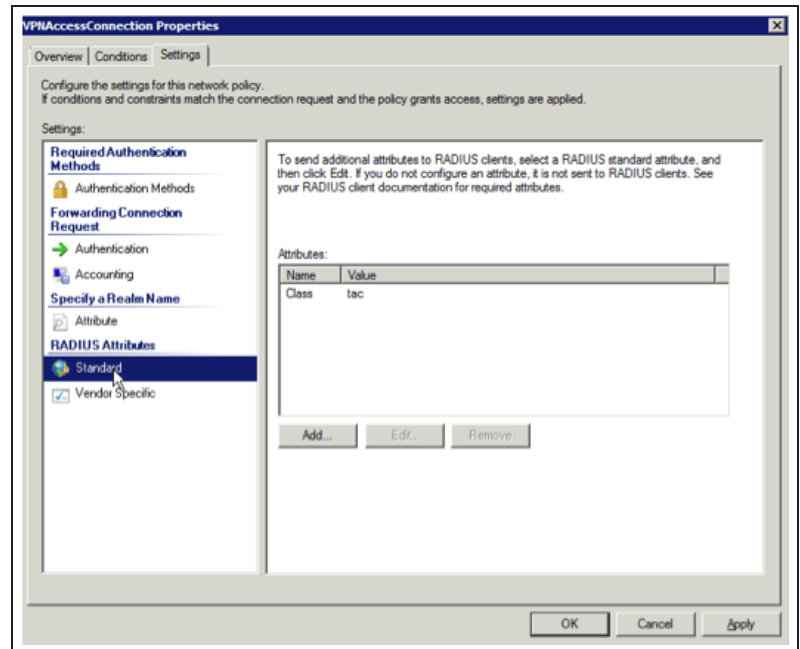
Add **Client IPv4 Address** and enter the IP of the FortiAP.



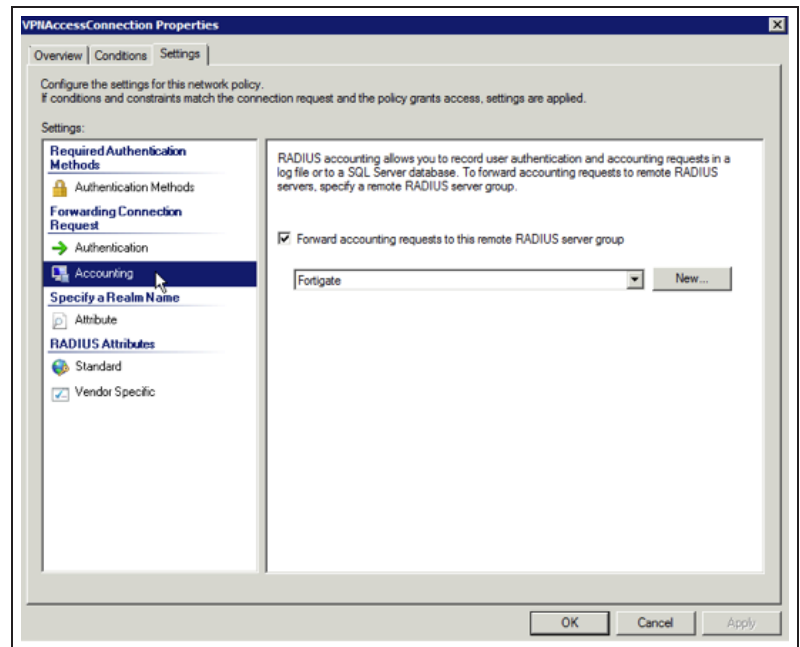


Go to **Settings**.

Select **RADIUS Attributes** and add the same class attribute used by the RSSO user group (in the example, *tac*).



Select **Accounting** and select **Forward accounting requests to the remote RADIUS server group**. Select the RADIUS server group from the list.



## 9. Results

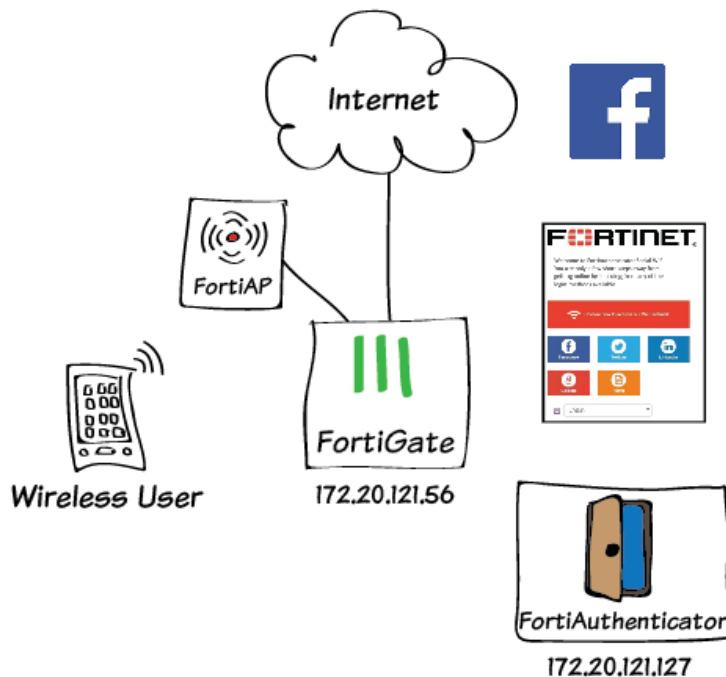
Users in the RSSO group will now be able to use their credentials to connect to the wireless network. They will then be able to access the Internet without having to authenticate again.

Go to **User & Device > Monitor > Firewall** to verify that users are able to connect to the FortiGate using RSSO.

| User Name | User Group | Duration                        | IP Address | Traffic Volume | Method |
|-----------|------------|---------------------------------|------------|----------------|--------|
| vale      | RSSO_Group | 0 day(s) 1 hour(s) 5 minute(s)  | 10.10.80.3 | N/A            | RSSO   |
| ipod      | RSSO_Group | 0 day(s) 0 hour(s) 52 minute(s) | 10.10.90.3 | 3.48 K         | RSSO   |

For further reading, check out [SSO using RADIUS accounting records](#) in the [FortiOS 5.2 Handbook](#).

# Social WiFi Captive Portal with FortiAuthenticator (Facebook)



WiFi authentication using social media provides access control without having to manually create guest accounts.

This recipe involves configuring an API for Facebook accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for Captive Portal access.

This recipe is similar to the **Captive portal WiFi access control**, but involves external security mode configuration, RADIUS authentication, and does not include FortiAP registration instructions.

Note that some CLI usage is required when configuring the FortiGate.

The FortiAuthenticator has been given an example fully qualified domain name (FQDN) – *fortiauthenticator.example.com*.

# 1. Configuring the Facebook developer account API

Open a browser and log in to your Facebook account.



In the URL field enter the following:

<https://developers.facebook.com/products/login/>

Select **My Apps** and select **Register as Developer**.

Confirm your Facebook password to continue.

Select that you have read and agree to the **Facebook Platform** and **Facebook Privacy** policies, and select **Next** to continue.

A screenshot of the 'Please re-enter your password' dialog box. At the top, the title 'Please re-enter your password' is in bold. Below it is a user profile picture and the name 'Wade Wilson'. The text says 'For your security, you must re-enter your password to continue.' followed by 'Password:' and a password input field. At the bottom, there is a link 'Forgotten your password?' and two buttons: 'Cancel' and 'Submit'.A screenshot of the 'Register as a Facebook Developer' dialog box. At the top, the title 'Register as a Facebook Developer' is in bold. Below it is a user profile picture and the name 'Wade Wilson'. The text asks 'Do you accept the Facebook Platform Policy and the Facebook Privacy Policy?'. To the right of the text are two radio buttons, with the 'YES' button selected and highlighted by a red rectangular box. At the bottom, there are two buttons: 'Cancel' and 'Next'.

Enter your phone number and select to have your confirmation code sent to you via text (you may also choose to verify via phone call).

Once received, enter the code and select **Register** to continue. You will now be registered as a Facebook developer.

Register as a Facebook Developer

We need to verify your account to complete your registration. Your Phone number will be added to your timeline but won't be visible to your friends.

Country

Canada (+1)

Phone number

877 234 1234

Get Confirmation Code

Send as Text

Send via Phone Call

Confirmation code

877 234

You can also verify your account by adding a credit card. [?]

Go Back

Register

Next, select the **Website** platform to add a new app.

Enter a name for the website, and select **Create New Facebook App ID**.

Add a New App

Select a platform to get started

Apple

iOS

Android

Android

Facebook

Facebook Canvas

WWW

Website

Start Over

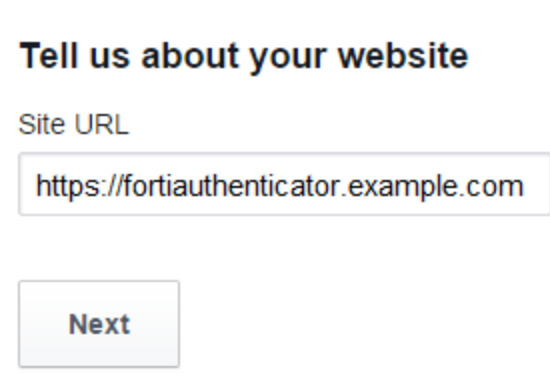
Skip and Create App ID

Quick Start for Website

fortiauthenticator.example.com

Create New Facebook App ID

Scroll down to the bottom of the page and enter the site's URL, then select **Next**. Scroll back up to the top of the page, and select **Skip Quick Start**.



**Tell us about your website**

Site URL

**Next**


Take note of the **App ID** and **App Secret** as they are required when configuring the Captive Portal on the FortiAuthenticator.

A screenshot of the Fortianalyzer web interface showing the "Basic" tab under the "fortiauthenticator...." header. The left sidebar contains navigation links: Dashboard, Settings (highlighted), Status & Review, App Details, Roles, Open Graph, Alerts, and Localize. The main area has three tabs: Basic, Advanced, and Migrations. Under the Basic tab, there are several fields: "App ID" (with value "67890ABCDEF"), "Display Name" (with value "fortiauthenticator.example.com"), "App Domains" (empty), "App Secret" (with value "XXXXXXXXXX-XXXXX-XXXXX-XXXXX-XXXXX"), "Namespace" (empty), "Contact Email" (empty), and "Site URL" (with value "https://<FAC\_FQDN>/"). A red box highlights the "App ID" field. Another red box highlights the "Display Name" field. A third red box highlights the "Site URL" field. There is also a "Reset" button next to the "App Secret" field and a "Quick Start" button at the bottom right.

Next, go to **Status & Review** and enable the application – the account needs to be made "live" before WiFi users can successfully authenticate through Facebook.

Status

Items in Review



fortiaauthenticator.example.com

Do you want to make this app and all its live features available to the general public?

YES

Submit Items for Approval

Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our [Platform Policy and Review Guidelines](#).

Start a Submission

Approved Items

LOGIN PERMISSIONS

email

Provides access to the person's primary email address. This permission is approved by default.

public\_profile

Provides access to a person's basic information, including first name, last name, profile picture, gender and age range. This permission is approved by default.

user\_friends

Provides access to a person's list of friends that also use your app. This permission is approved by default.

The **App ID** and **App Secret** can be accessed at any time on the LinkedIn developer account, but it may be a good idea to copy them to a secure location.

570

WiFi

## 2. Configuring the social portal RADIUS service on FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > User Groups**, and create a **Social\_Users** user group.

Users that log into LinkedIn will be placed in this group once it is added to the Captive Portal General Settings.

The screenshot shows the 'Social\_Users' user group configuration page. The 'Name' field is 'Social\_Users'. The 'Type' is 'Local'. The 'Users' section shows a list of 'Available users' and a 'Selected users' list. The 'RADIUS Attributes' table is empty. The 'Add Attribute' button is visible. The 'OK' and 'Cancel' buttons are at the bottom.

Go to **Authentication > RADIUS Service > Clients**, and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enable the **Social portal** captive portal.

The screenshot shows the 'RADIUS Client' configuration page. The 'Name' is 'RADIUSclient'. The 'Client name IP' is '172.20.121.56'. The 'Secret' is masked. The 'Enable captive portal' section has 'Social portal (URL: /social\_login)' checked. The 'Profiles' section shows a list of profiles, with 'Default' selected. The 'Authentication method' is 'Password-only authentication'. The 'Username input format' is 'realmusername'. The 'Realms' table shows a list of realms, with 'local | Local users' selected. The 'Groups' column shows 'Social\_Users (0:0)' and 'Filter local users: 0:0'. The 'Save' button is at the bottom.

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Add the **Social\_Users** user group to the **Realms** group filter as shown.

Select **Save** and then **OK**.

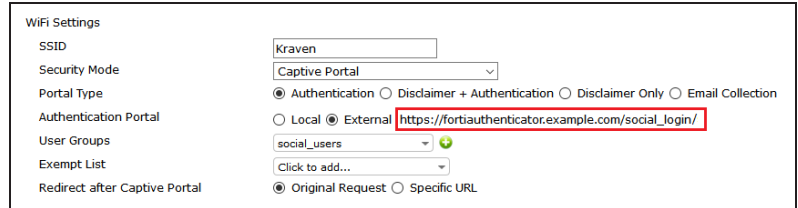




## 4. Configuring the FortiGate WiFi settings

Go to **WiFi & Switch Controller > WiFi Network > SSID** and select the SSID interface.

Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.



|                               |   |
|-------------------------------|---|
| WiFi Settings                 |   |
| SSID                          | Kraven  |
| Security Mode                 | Captive Portal  |
| Portal Type                   | <input checked="" type="radio"/> Authentication <input type="radio"/> Disclaimer + Authentication <input type="radio"/> Disclaimer Only <input type="radio"/> Email Collection                |
| Authentication Portal         | <input type="radio"/> Local <input checked="" type="radio"/> External <a href="https://fortiauthenticator.example.com/social_login/">https://fortiauthenticator.example.com/social_login/</a> |
| User Groups                   | social_users  |
| Exempt List                   | Click to add...   |
| Redirect after Captive Portal | <input checked="" type="radio"/> Original Request <input type="radio"/> Specific URL  |

For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social\_login/**.

For this recipe, it is set to:

`https://fortiauthenticator.example.com/social_login/`

Set **User Groups** to the **social\_users** group.

## 5. Configuring the FortiGate to allow access to Facebook

On the FortiGate, configure firewall addresses to allow users to access the Facebook login page.

The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can also copy and paste the commands below into the CLI console.

Go to **System > Dashboard** and enter the **CLI Console**. Enter the following, which creates the firewall addresses and adds them to a firewall address group called **Facebook\_Auth**:

```
config firewall address
  edit "FB0"
    set subnet 5.178.32.0 255.255.240.0
  next
  edit "FB1"
    set subnet 195.27.154.0 255.255.255.0
  next
  edit "FB2"
    set subnet 80.150.154.0 255.255.255.0
  edit "FB3"
    set subnet 77.67.96.0 255.255.252.0
  next
  edit "FB4"
    set subnet 212.119.27.0 255.255.255.128
  next
```

```

edit "FB5"
  set subnet 2.16.0.0 255.248.0.0
next
edit "FB6"
  set subnet 66.171.231.0 255.255.255.0
next
edit "FB7"
  set subnet 31.13.24.0 255.255.248.0
next
edit "FB8"
  set subnet 31.13.64.0 255.255.192.0
next
edit "FB9"
  set subnet 23.67.246.0 255.255.255.0
next
edit "akamai-subnet-23.74.8"
  set subnet 23.74.8.0 255.255.255.0
next
edit "akamai-subnet-23.74.9"
  set subnet 23.74.9.0 255.255.255.0
next edit "akamaihd.net"
  set type fqdn      set fqdn "akamaihd.net"
next
edit "channel-proxy-06-frc1.facebook.com"
  set type fqdn
  set fqdn "channel-proxy-06-frc1.facebook.com"
next
edit "code.jquery.com"
  set type fqdn
  set fqdn "code.jquery.com"
next
edit "connect.facebook.com"
  set type fqdn
  set fqdn "connect.facebook.com"
next
edit "fbcdn-photos-c-a.akamaihd.net"
  set type fqdn
  set fqdn "fbcdn-photos-c-a.akamaihd.net"
next
edit "fbcdn-profile-a.akamaihd.net"
  set type fqdn
  set fqdn "fbcdn-profile-a.akamaihd.net"
next edit "fbexternal-a.akamaihd.net"
  set type fqdn
  set fqdn "fbexternal-a.akamaihd.net"
next
edit "fbstatic-a.akamaihd.net"
  set type fqdn
  set fqdn "fbstatic-a.akamaihd.net"

```

```

next
edit "m.facebook.com"
    set type fqdn
    set fqdn "m.facebook.com"
next
edit "ogp.me"
    set type fqdn
    set fqdn "ogp.me" next
edit "s-static.ak.facebook.com"
    set type fqdn
    set fqdn "s-static.ak.facebook.com"
next
edit "static.ak.facebook.com"
    set type fqdn
    set fqdn "static.ak.facebook.com"
next
edit "static.ak.fbcdn.com"
    set type fqdn    set fqdn "static.ak.fbcdn.com"
next
edit "web_ext_addr_SocialWiFi"
    set type fqdn
    set fqdn "web_ext_addr_SocialWiFi"
next
edit "www.facebook.com"
    set type fqdn
    set fqdn "www.facebook.com"
next
end

config firewall addrgrp
edit "Facebook Auth"
    set member "FB0" "FB1" "FB2" "FB3" "FB4" "FB5" "FB6" "FB7" "FB8" "FB9"
        "akamaisubnet-23.74.8" "akamai-subnet-23.74.9" "akamaihd.net"
        "channel-proxy-06-frcl.facebook.com" "code.jquery.com"
        "connect.facebook.com" "fbcdn-photos-ca.akamaihd.net"
        "fbcdn-profile-a.akamaihd.net" "fbexternal-a.akamaihd.net"
        "fbstatic-a.akamaihd.net" "m.facebook.com" "ogp.me"
        "s-static.ak.facebook.com" "static.ak.facebook.com"
        "static.ak.fbcdn.com" "web_ext_addr_SocialWiFi"
        "www.facebook.com" "FortiAuthenticator"

next
end

```

Go to **Policy & Objects > Policy > IPv4** and create a policy for Facebook authentication traffic.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Facebook\_Auth**.

Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.

|   |                                     |
|---|-------------------------------------|
| Incoming Interface  | wifi (SSID: Kraven)                 |
| Source Address  | all                                 |
| Source User(s)  | Click to add...                     |
| Source Device Type  | Click to add...                     |
| Outgoing Interface  | wan1                                |
| Destination Address   | Facebook_Auth                       |
| Schedule  | always                              |
| Service   | ALL                                 |
| Action  | ACCEPT                              |
| <b>Firewall / Network Options</b>                               |                                     |
| <input checked="" type="checkbox"/> NAT                         |                                     |
| <input checked="" type="radio"/> Use Outgoing Interface Address | <input type="checkbox"/> Fixed Port |
| <input type="radio"/> Use Dynamic IP Pool                       | Click to add...                     |
| <input type="radio"/> Use Central NAT Table                     |                                     |

Go to **System > Dashboard** and enter the **CLI Console**. Add the following to exempt the Facebook authentication traffic policy from the captive portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

This command allows access to the external Captive Portal.

## 6. Configuring the FortiGate to allow access to FortiAuthenticator

On the FortiGate, go to **Policy & Objects > Objects > Addresses** and add the FortiAuthenticator firewall object.

For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | FortiAuthenticator  |
| Type                 | IP/Netmask  |
| Subnet / IP Range    | 172.20.121.127  |
| Interface            | any   |
| Show in Address List | <input checked="" type="checkbox"/>   |

Go to **Policy & Objects > Policy > IPv4** and create the FortiAuthenticator access policy.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **FortiAuthenticator**.

Set **Service** to **ALL** and enable **NAT**.

|  |                     |
|--|---------------------|
| Incoming Interface                         | wifi (SSID: Kraven) |
| Source Address                             | all                 |
| Source User(s)                             | Click to add...     |
| Source Device Type                         | Click to add...     |
| Outgoing Interface                         | wan1                |
| Destination Address                        | FortiAuthenticator  |
| Schedule                                   | always              |
| Service                                    | ALL                 |
| Action                                     | ACCEPT              |
| <b>Firewall / Network Options</b>          |                     |
| <input checked="" type="checkbox"/> ON NAT |                     |

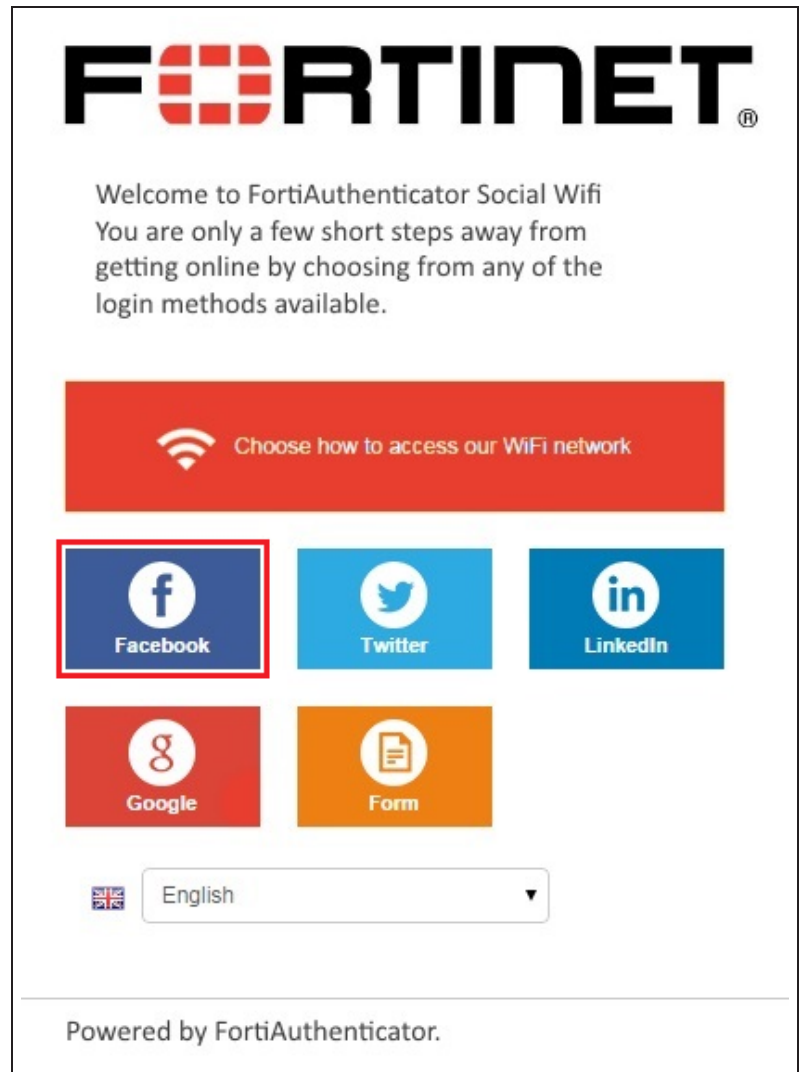
Add the following to exempt the FortiAuthenticator access policy from the Captive Portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

## 7. Results

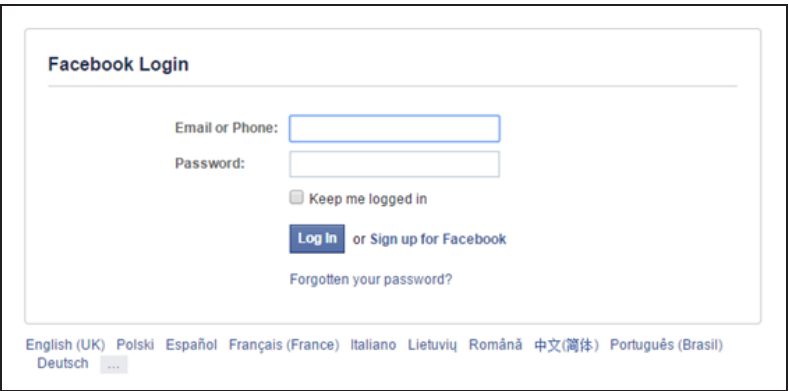
Connect to the WiFi and attempt to browse the Internet. You will be redirected to the Captive Portal splash page.

Select **Facebook** and you should be redirected to the Facebook login page.



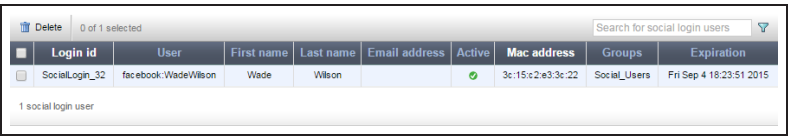
Enter valid Facebook credentials and you will be redirected to the URL initially requested.

You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



The image shows a Facebook Login page. It has a title "Facebook Login" at the top. Below the title, there are two input fields: "Email or Phone:" and "Password:". Below the password field, there is a checkbox labeled "Keep me logged in". Below the checkbox, there are two buttons: "Log In" and "or Sign up for Facebook". Below the buttons, there is a link "Forgotten your password?". At the bottom, there is a row of language options: English (UK), Polski, Español, Français (France), Italiano, Lietuvių, Română, 中文(简体), Português (Brasil), and Deutsch.

To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.



The image shows a table of Social Login Users. The table has columns: Login id, User, First name, Last name, Email address, Active, Mac address, Groups, and Expiration. There is one row of data. Below the table, it says "1 social login user".

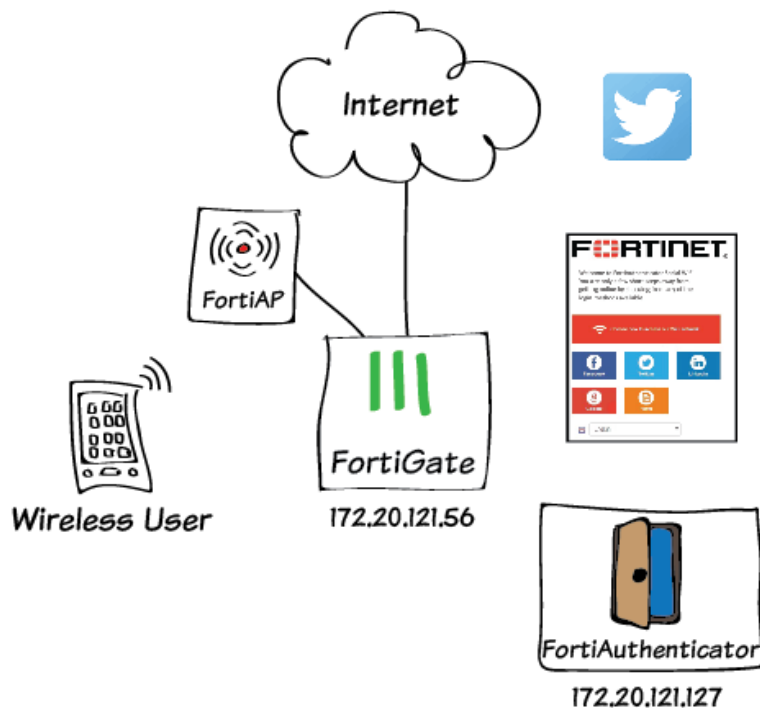
| Login id       | User                | First name | Last name | Email address | Active | Mac address       | Groups       | Expiration              |
|----------------|---------------------|------------|-----------|---------------|--------|-------------------|--------------|-------------------------|
| SocialLogin_32 | facebook:WadeWilson | Wade       | Wilson    |               | ✓      | 3c:15:c2:e3:3c:22 | Social_Users | Fri Sep 4 18:23:51 2015 |

You can configure Captive Portal to use other social WiFi logins:

- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)



# Social WiFi Captive Portal with FortiAuthenticator (Twitter)



WiFi authentication using social media provides access control without having to manually create guest accounts.

This recipe involves configuring an API for Twitter accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for Captive Portal access.

This recipe is similar to the **Captive portal WiFi access control**, but involves external security mode configuration, RADIUS authentication, and does not include FortiAP registration instructions.

Note that some minimal CLI usage is required when configuring the FortiGate.

The FortiAuthenticator has been given an example fully qualified domain name (FQDN) – *fortiauthenticator.example.com*.

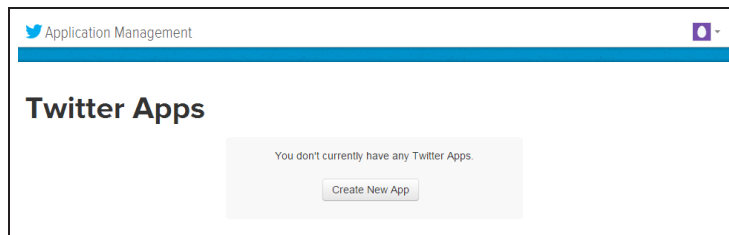
A recipe of this video is available [here](#).

# 1. Configuring the Twitter developer account API

Open a browser and log in to your Twitter account. In the URL field enter the following:

<https://apps.twitter.com/>

Select **Create New App**.



Enter a **Name**, **Description**, and **Website** for the application.

In the **Callback URL** field, enter the following:

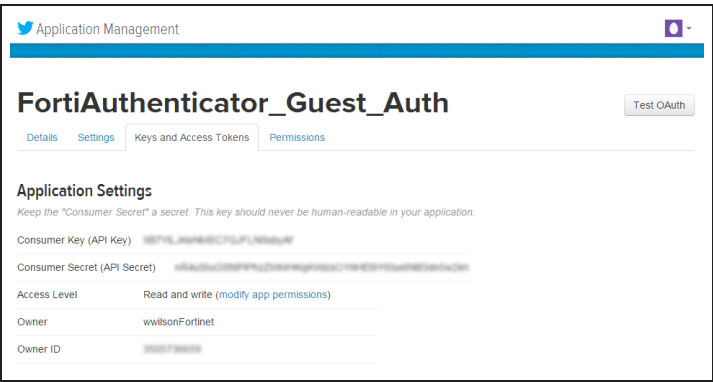
<https://fortiauthenticator.example.com/social/complete/twitter/>

Note that the FortiAuthenticator needs to be able to access the Internet.

Accept the Developer Agreement and select **Create your Twitter application**.

Go to **Keys and Access Tokens** to view your **Consumer Key** and **Consumer Secret**.

Take note of the **Consumer Key** and **Consumer Secret** as they are required when configuring the Captive Portal on the FortiAuthenticator.

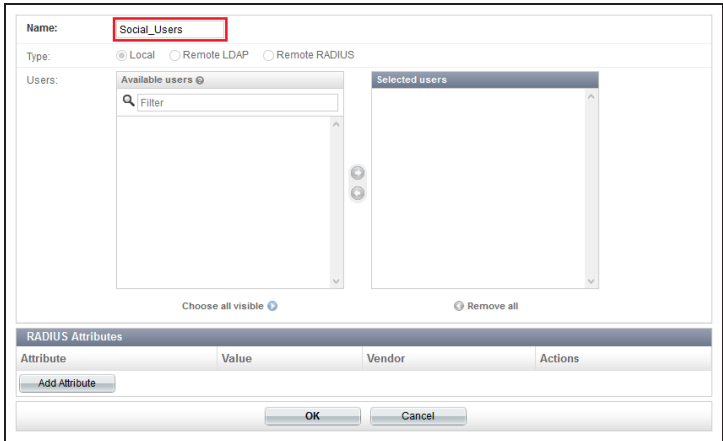


The **Consumer Key** and **Consumer Secret** can be accessed at any time on the Twitter developer account, but it may be a good idea to copy them to a secure location.

## 2. Configuring the social portal RADIUS service on FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > User Groups**, and create a **Social\_Users** user group.

Users that log into Twitter will be placed in this group once it is added to the Captive Portal General Settings.



Go to **Authentication > RADIUS Service > Clients**, and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enable the **Social portal** captive portal.

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Add the **Social\_Users** user group to the **Realms** group filter as shown.

Select **Save** and then **OK**.

Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.

Configure the account expiry time (in the example it is set to 1 hour).

Set **Place registered users into a group** to **Social\_Users**.

Enable the **Twitter** login option and add your **Twitter Consumer Key** and **Consumer Secret**.

### 3. Configuring the FortiGate authentication settings

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.

Use the **Test Connectivity** option with valid credentials to test the connection.

The screenshot shows the configuration for a RADIUS server named 'FAC-RADIUS'. The primary server IP is 172.20.121.127. There are two 'Test Connectivity' buttons. The authentication method is set to 'Default'. The NAS IP / Called Station ID field is empty. The 'Include in every User Group' checkbox is unchecked.

Next, go to **User & Device > User > User Groups** and create a RADIUS user group called **social\_users**.

Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

The screenshot shows the configuration for a user group named 'social\_users'. The type is set to 'Firewall'. The 'Remote groups' table lists 'FAC-RADIUS' as a remote server with the group name 'Any'.

### 4. Configuring the FortiGate WiFi settings

Go to **WiFi & Switch Controller > WiFi Network > SSID** and select the SSID interface.

Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.

The screenshot shows the WiFi settings for an SSID named 'Kraven'. The security mode is 'Captive Portal'. The authentication portal is set to 'External' with the URL 'https://fortiauthenticator.example.com/social\_login/'. The user groups are set to 'social\_users'. The redirect after captive portal is set to 'Original Request'.

For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social\_login/**.

For this recipe, it is set to:  
`https://fortiauthenticator.example.com/social_login/`

Set **User Groups** to the **social\_users** group.

### 5. Configuring the FortiGate to allow access to Twitter

On the FortiGate, configure firewall addresses to allow users to access the Twitter login page.

The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can also copy and paste the commands below into the CLI console.

Go to **System > Dashboard** and enter the **CLI Console**. Enter the following, which creates the firewall addresses and adds them to a firewall address group called **Twitter\_Auth**:

```
config firewall address
  edit "api.twitter.com"
    set type fqdn
    set fqdn "api.twitter.com"
  next
  edit "abs.twimg.com"
    set type fqdn
    set fqdn "abs.twimg.com"
  next
  edit "abs-0.twimg.com"
    set type fqdn
    set fqdn "abs-0.twimg.com"
  next
end

config firewall addgrp
  edit "Twitter_Auth"
    set member "api.twitter.com" "abs.twimg.com" "abs-0.twimg.com"
  next
end
```

Go to **Policy & Objects > Policy > IPv4** and create a policy for Twitter authentication traffic.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Twitter\_Auth**.

Set **Service** to **ALL** and enable NAT. Configure **Security Profiles** accordingly.



|                                   |                     |
|-----------------------------------|---------------------|
| Incoming Interface                | wifi (SSID: Kraven) |
| Source Address                    | all                 |
| Source User(s)                    | Click to add...     |
| Source Device Type                | Click to add...     |
| Outgoing Interface                | wan1                |
| Destination Address               | Twitter_Auth        |
| Schedule                          | always              |
| Service                           | ALL                 |
| Action                            | ACCEPT              |
| <b>Firewall / Network Options</b> |                     |
| ON NAT                            |                     |

Go to **System > Dashboard** and enter the **CLI Console**. Add the following to exempt the Twitter authentication traffic policy from the captive portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

This command allows access to the external Captive Portal.

## 6. Configuring the FortiGate to allow access to FortiAuthenticator

On the FortiGate, go to **Policy & Objects > Objects > Addresses** and add the FortiAuthenticator firewall object.

For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | FortiAuthenticator  |
| Type                 | IP/Netmask  |
| Subnet / IP Range    | 172.20.121.127  |
| Interface            | any   |
| Show in Address List | <input checked="" type="checkbox"/>   |

Go to **Policy & Objects > Policy > IPv4** and create the FortiAuthenticator access policy.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to all.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to FortiAuthenticator.

Set **Service** to ALL and enable NAT.

|   |                     |
|---|---------------------|
| Incoming Interface                      | wifi (SSID: Kraven) |
| Source Address                          | all                 |
| Source User(s)                          | Click to add...     |
| Source Device Type                      | Click to add...     |
| Outgoing Interface                      | wan1                |
| Destination Address                     | FortiAuthenticator  |
| Schedule                                | always              |
| Service                                 | ALL                 |
| Action                                  | ACCEPT              |
| <b>Firewall / Network Options</b>       |                     |
| <input checked="" type="checkbox"/> NAT |                     |

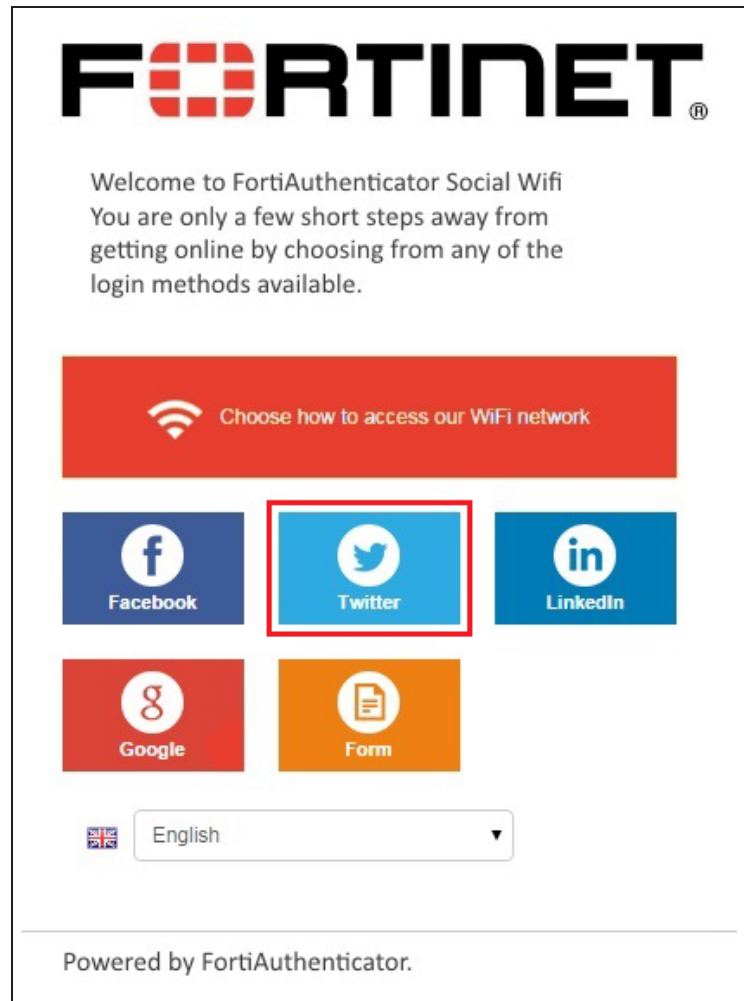
Add the following to exempt the FortiAuthenticator access policy from the Captive Portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

## 7. Results

Connect to the WiFi and attempt to browse the Internet. You will be redirected to the Captive Portal splash page.

Select **Twitter** and you should be redirected to the Twitter login page.





Enter valid Twitter credentials and you will be redirected to the URL initially requested.

You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.

Authorize

FortiAuthenticator\_Guest\_Auth to use your account?

Username or email

fortiauthenticator.example.com

Password

Social authenticate WiFi users into FSSO

☐ Remember me · [Forgot password?](#)

Sign In

Cancel

This application will be able to:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

Will not be able to:

- Access your direct messages.
- See your Twitter password.

To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

Delete0 of 1 selected

Search for social login users

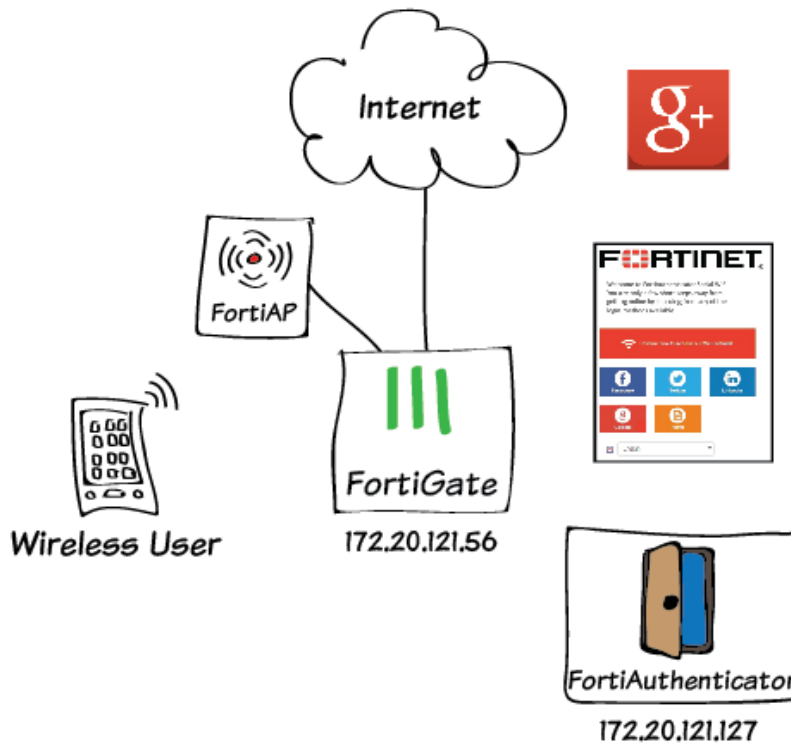
|                          | Login id       | User                    | First name | Last name | Email address | Active                              | Mac address       | Groups       | Expiration              |
|--------------------------|----------------|-------------------------|------------|-----------|---------------|-------------------------------------|-------------------|--------------|-------------------------|
| <input type="checkbox"/> | SocialLogin_40 | twitter.wilson@Fortinet | Wade       | Wilson    |               | <input checked="" type="checkbox"/> | 3c:15:c2:e3:3c:22 | Social_Users | Wed Sep 9 17:16:03 2015 |

1 social login user

You can configure Captive Portal to use other social WiFi logins:

- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)

# Social WiFi Captive Portal with FortiAuthenticator (Google+)



WiFi authentication using social media provides access control without having to manually create guest accounts.

This recipe involves configuring an API for Google+ accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for Captive Portal access.

This recipe is similar to the [Captive portal WiFi access control](#), but involves external security mode configuration, RADIUS authentication, and does not include FortiAP registration instructions.

Note that some minimal CLI usage is required when configuring the FortiGate.

The FortiAuthenticator has been given an example fully qualified domain name (FQDN) – *fortiauthenticator.example.com*.

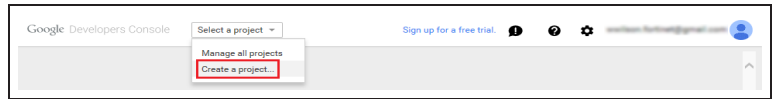
## 1. Configuring the Google+ developer account API

Open a browser and log in to your Google account. In the URL field enter the following:

<https://console.developers.google.com>

Under **Select a project**, select **Create a project**.

Enter a **Project name**, and accept the **Terms of Service** before continuing.



**New Project**

**Project name** ?

FortiAuthenticator

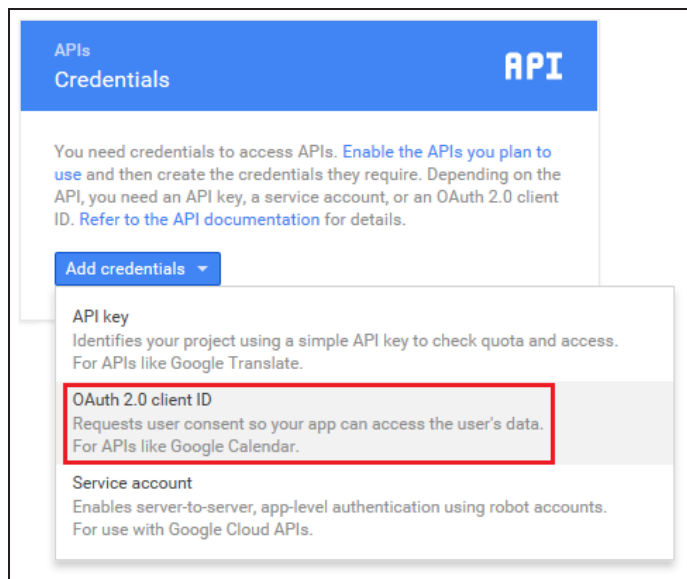
Your project ID will be fortiauthenticator-1051 ? [Edit](#)

[Show advanced options...](#)

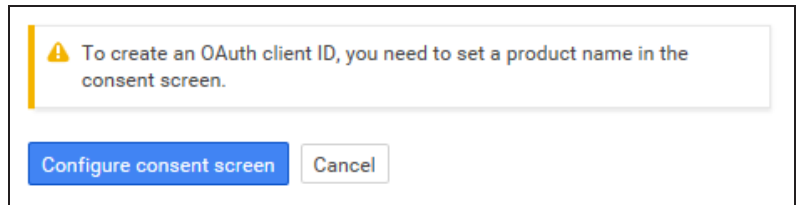
☒ I agree that my use of any [services and related APIs](#) is subject to my compliance with the applicable [Terms of Service](#).

[Create](#) [Cancel](#)

Go to **APIs & auth > Credentials**, and select **OAuth 2.0 client ID** from the **Add credentials** dropdown.



When prompted, select **Configure consent screen**. Enter an **Email address** and **Product name**. You must now create the client ID.



Set Application type to Web application. Under Authorized JavaScript origins, enter the FortiAuthenticator FQDN.

Under **Authorized redirect URIs**, enter the following:

`https://fortiauthenticator.example.com/social/complete/google-oauth2/`

Note that the FortiAuthenticator needs to be able to access the Internet.

Upon creating the client ID, a window will appear with your **client ID** and **client secret**.

Take note of the **client ID** and **client secret** as they are required when configuring the Captive Portal on the FortiAuthenticator.

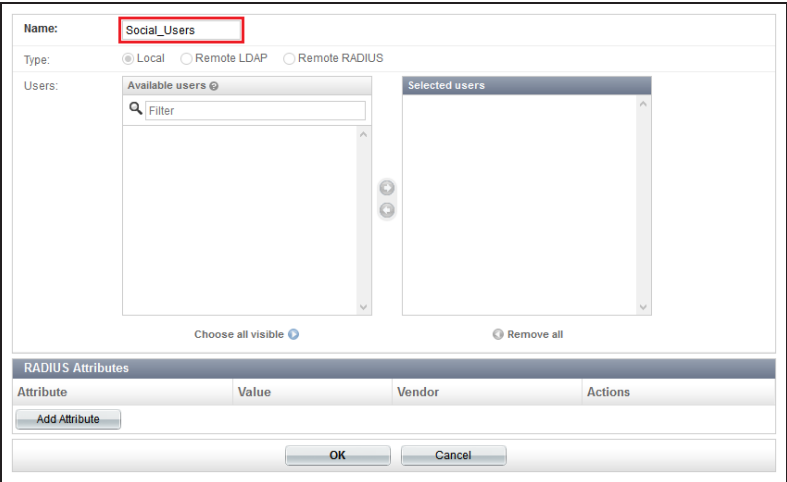


The **client ID** and **client secret** can be accessed at any time on the Google developer account, but it may be a good idea to copy them to a secure location.

## 2. Configuring the social portal RADIUS service on FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > User Groups**, and create a **Social\_Users** user group.

Users that log into Google will be placed in this group once it is added to the Captive Portal General Settings.



Go to **Authentication > RADIUS Service > Clients**, and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enable the **Social portal** captive portal.

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Add the **Social\_Users** user group to the **Realms** group filter as shown.

Select **Save** and then **OK**.

Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.

Configure the account expiry time (in the example it is set to 1 hour).

Set **Place registered users into a group** to **Social\_Users**.

Enable the **Google** login option and add your **Google key** and **Google secret**.

### 3. Configuring the FortiGate authentication settings

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.

Use the **Test Connectivity** option with valid credentials to test the connection.

Name

FAC-RADIUS

Primary Server IP/Name

172.20.121.127

Primary Server Secret

••••••••

Test Connectivity

Secondary Server IP/Name

Secondary Server Secret

Test Connectivity

Authentication Method

☒ Default ☐ Specify

NAS IP / Called Station ID

Include in every User Group

☐

Next, go to **User & Device > User > User Groups** and create a RADIUS user group called **social\_users**.

Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Name

social\_users

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

Click to add...

Remote groups

Create New Edit Delete

| Remote Server | Group Name |
|---------------|------------|
| FAC-RADIUS    | Any        |

### 4. Configuring the FortiGate WiFi settings

Go to **WiFi & Switch Controller > WiFi Network > SSID** and select the SSID interface.

Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.

WiFi Settings

SSID

Kraven

Security Mode

Captive Portal

Portal Type

☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal

☐ Local ☒ External 

https://fortiauthenticator.example.com/social\_login/

User Groups

social\_users

Exempt List

Click to add...

Redirect after Captive Portal

☒ Original Request ☐ Specific URL

For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social\_login/**.

For this recipe, it is set to:  
`https://fortiauthenticator.example.com/social_login/`

Set **User Groups** to the **social\_users** group.

## 5. Configuring the FortiGate to allow access to Google

On the FortiGate, configure firewall addresses to allow users to access the Google login page.

The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can also copy and paste the commands below into the CLI console.

Go to **System > Dashboard** and enter the **CLI Console**. Enter the following, which creates the firewall addresses and adds them to a firewall address group called **Google\_Auth**:

```
config firewall address
  edit "www.googleapis.com"
    set type fqdn
    set fqdn "www.googleapis.com"
  next
  edit "accounts.google.com"
    set type fqdn    set fqdn "accounts.google.com"
  next
  edit "ssl.gstatic.com"
    set type fqdn
    set fqdn "ssl.gstatic.com"
  next
  edit "fonts.gstatic.com"
    set type fqdn
    set fqdn "fonts.gstatic.com"
  next
  edit "www.gstatic.com"
    set type fqdn
    set fqdn "www.gstatic.com"
  next
  edit "Google_13"
    set subnet 216.58.192.0 255.255.224.0
  next
end

config firewall addrgrp
  edit "Google_Auth"
    set member "ssl.gstatic.com" "accounts.google.com" "www.googleapis.com"
    set member "fonts.gstatic.com" "www.gstatic.com" "Google_13"
  next
end
```



Go to **Policy & Objects > Policy > IPv4** and create a policy for Google authentication traffic.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **Google\_Auth**.

Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.

|                     |                     |   |
|---------------------|---------------------|---|
| Incoming Interface  | wifi (SSID: Kraven) | + |
| Source Address      | all                 | + |
| Source User(s)      | Click to add...     |   |
| Source Device Type  | Click to add...     |   |
| Outgoing Interface  | wan1                | + |
| Destination Address | Google_Auth         | + |
| Schedule            | always              |   |
| Service             | ALL                 | + |
| Action              | ACCEPT              |   |

**Firewall / Network Options**

☒ ON NAT

Go to **System > Dashboard** and enter the **CLI Console**. Add the following to exempt the Google authentication traffic policy from the captive portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

This command allows access to the external Captive Portal.

## 6. Configuring the FortiGate to allow access to FortiAuthenticator

On the FortiGate, go to **Policy & Objects > Objects > Addresses** and add the FortiAuthenticator firewall object.

For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | FortiAuthenticator  |
| Type                 | IP/Netmask  |
| Subnet / IP Range    | 172.20.121.127  |
| Interface            | any   |
| Show in Address List | <input checked="" type="checkbox"/>   |

Go to **Policy & Objects > Policy > IPv4** and create the FortiAuthenticator access policy.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **FortiAuthenticator**.

Set **Service** to **ALL** and enable **NAT**.

|                     |                     |
|---------------------|---------------------|
| Incoming Interface  | wifi (SSID: Kraven) |
| Source Address      | all                 |
| Source User(s)      | Click to add...     |
| Source Device Type  | Click to add...     |
| Outgoing Interface  | wan1                |
| Destination Address | FortiAuthenticator  |
| Schedule            | always              |
| Service             | ALL                 |
| Action              | ACCEPT              |

**Firewall / Network Options**  
☒ NAT

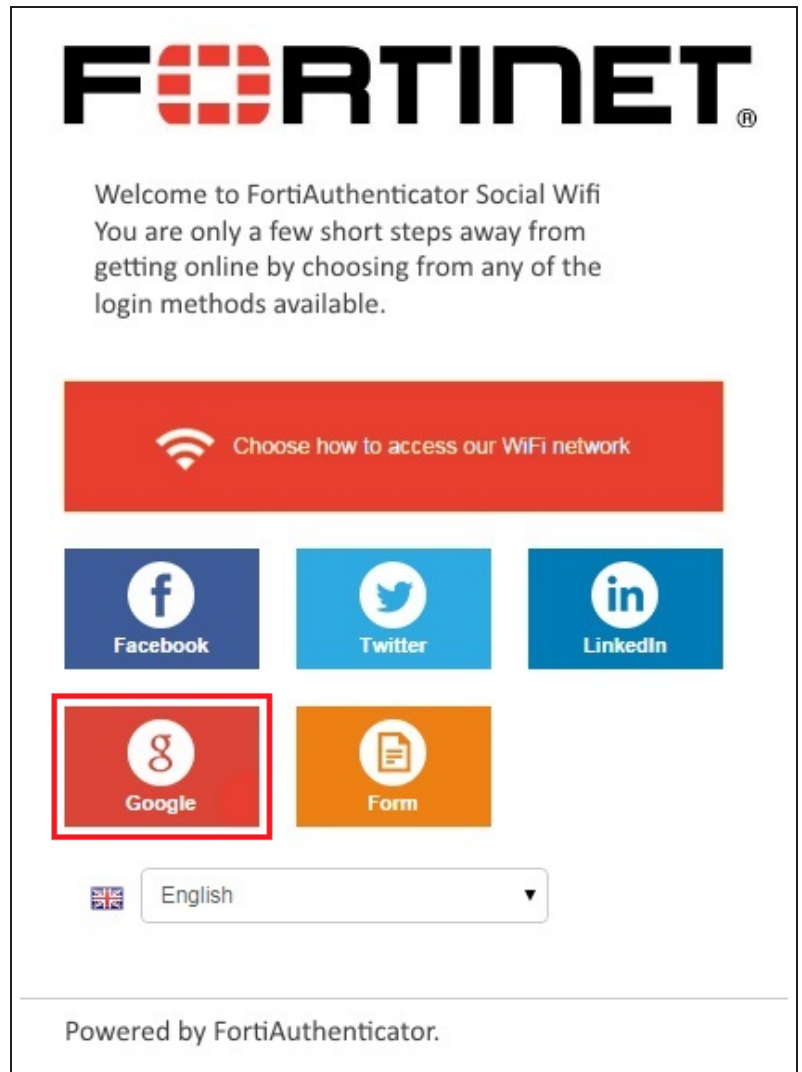
Add the following to exempt the FortiAuthenticator access policy from the Captive Portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

## 7. Results

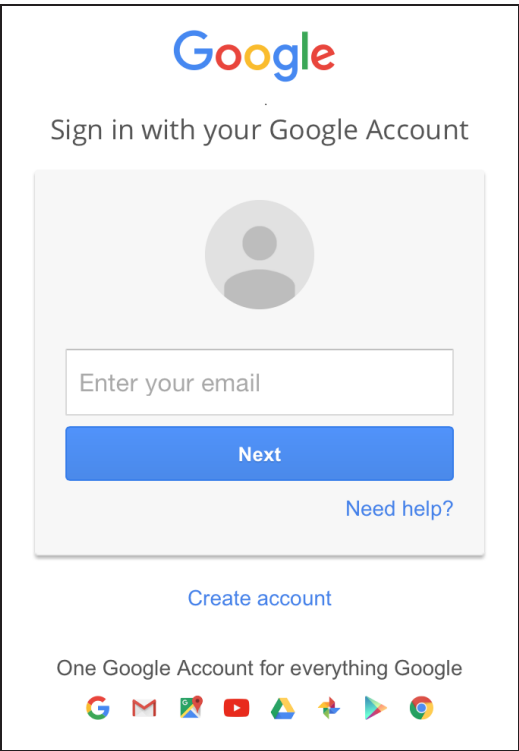
Connect to the WiFi and attempt to browse the Internet. You will be redirected to the Captive Portal splash page.

Select **Google** and you should be redirected to the Google login page.






Enter valid Google credentials and you will be redirected to the URL initially requested.

You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



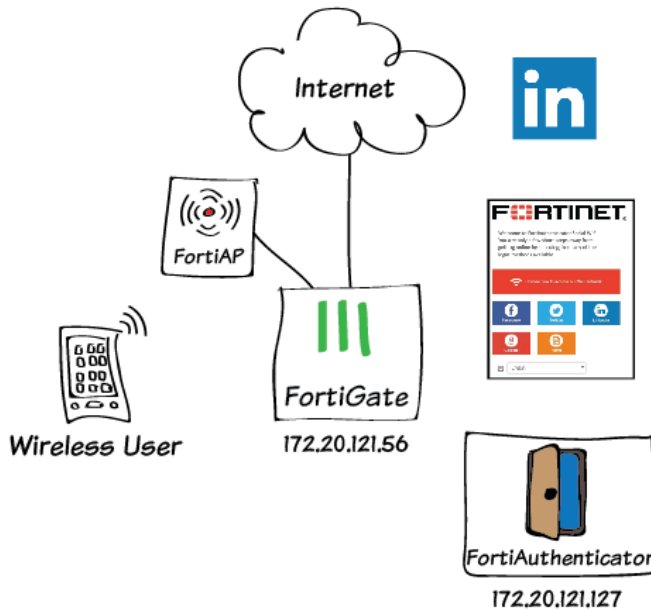
To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

|  Delete |                | 0 of 1 selected         |            |           |                            |   | <input type="text" value="Search for social login users"/> |              |                         |  |
|--|----------------|-------------------------|------------|-----------|----------------------------|---|--|--------------|-------------------------|---|
| <input type="checkbox"/>   | Login id       | User                    | First name | Last name | Email address              | Active  | Mac address  | Groups       | Expiration              |   |
| <input type="checkbox"/>   | SocialLogin_33 | google:wwilson.fortinet | Wade       | Wilson    | wwilson.fortinet@gmail.com |  | 3c:15:c2:e3:3c:22  | Social_Users | Fri Sep 4 18:30:52 2015 |   |
| 1 social login user  |                |                         |            |           |                            |   |  |              |                         |   |

You can configure Captive Portal to use other social WiFi logins:

- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)

# Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)



WiFi authentication using social media provides access control without having to manually create guest accounts.

This recipe involves configuring an API for LinkedIn accounts, setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for Captive Portal access.

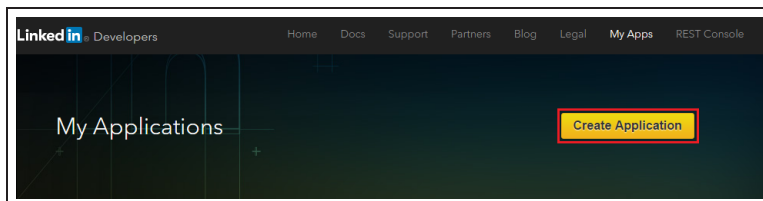
This recipe is similar to the **Captive portal WiFi access control** recipe, but involves external security mode configuration, RADIUS authentication, and does not include FortiAP registration instructions.

Note that some minimal CLI usage is required when configuring the FortiGate.

The FortiAuthenticator has been given an example fully qualified domain name (FQDN) – *fortiauthenticator.example.com*.

## 1. Configuring the LinkedIn developer account API

Open a browser and log in to your LinkedIn account.



In the URL field enter the following:

<https://developer.linkedin.com/documents/authentication>

Select **Create Application**.

Enter information in the required fields. Unlike the other social applications, LinkedIn requires an Application Logo URL.

Select that you have read and agree to the [LinkedIn API Terms if Use](#) and select **Submit**.

### Create a New Application

**Company Name: \***

**Name: \***

**Description: \***

**Application Logo URL: \***

**Application Use:\***

Communications ▼

**Website URL:\***

http://www.fortinet.com

**Business Email:\***

wwilson@fortinet.com

**Business Phone:\***

123-456-7890

☒ I have read and agree to the [LinkedIn API Terms of Use](#).

Submit

Cancel

The next screen shows your **Client ID** and **Client secret**.

Take note of the **Client ID** and **Client secret** as they are required when configuring the Captive Portal on the FortiAuthenticator.

Authentication Keys

Client ID:

Client Secret:

Default Application Permissions

☒ r\_basicprofile ☐ r\_emailaddress ☐ rw\_company\_admin  
☐ w\_share

OAuth 2.0

Authorized Redirect URLs:

OAuth 1.0a

Default "Accept" Redirect URL:

Default "Cancel" Redirect URL:

Under **Authorized Redirect URLs**, enter the following:  
`https://fortiauthenticator.example.com/social/complete/linkedin-oauth2/`

Note that the FortiAuthenticator needs to be able to access the Internet.

The **client ID** and **client secret** can be accessed at any time on the LinkedIn developer account, but it may be a good idea to copy them to a secure location.



## 2. Configuring the social portal RADIUS service on FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > User Groups**, and create a **Social\_Users** user group.

Users that log into LinkedIn will be placed in this group once it is added to the Captive Portal General Settings.

The screenshot shows the 'Social\_Users' user group configuration page. The 'Name' field is 'Social\_Users' and is highlighted with a red box. The 'Type' is set to 'Local'. The 'Users' section shows 'Available users' and 'Selected users' lists. The 'RADIUS Attributes' table is empty. The 'OK' button is highlighted.

Go to **Authentication > RADIUS Service > Clients**, and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enable the **Social portal** captive portal.

The screenshot shows the 'RADIUS Client' configuration page. The 'Name' is 'RADIUSclient' and the 'Client name/IP' is '172.20.121.56'. The 'Secret' is masked. The 'Enable captive portal' section has 'Social portal (URL: /social\_login)' checked. The 'Profiles' section shows a 'Default' profile with 'Authentication method' set to 'Password-only authentication'. The 'Username input format' is 'username@realm'. The 'Realms' table has a row for 'local / Local users' with a filter 'Social\_Users'. The 'Save' button is highlighted.

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Add the **Social\_Users** user group to the **Realms** group filter as shown.

Select **Save** and then **OK**.

Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.

Configure the account expiry time (in the example it is set to 1 hour).

Set **Place registered users into a group** to **Social\_Users**.

Enable the **LinkedIn** login option and add your **LinkedIn key** and **LinkedIn secret**.

**Social Portal**

☒ Enable social portal (URL: /social\_login/)

☐ Enable disclaimer

☒ Account expires after

1

hour(s)

☒ Place registered users into a group

Social\_Users

☐ Enable Facebook login

☐ Enable Google login

☐ Enable Twitter login

☒ Enable LinkedIn login

LinkedIn key:

LinkedIn secret:

☐ Enable SMS self-registration

☐ Enable e-mail self-registration

**MAC Address Portal**

☐ Enable MAC address portal (URL: /malogin/)

OK

### 3. Configuring the FortiGate authentication settings

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.

Use the **Test Connectivity** option with valid credentials to test the connection.

Name

FAC-RADIUS

Primary Server IP/Name

172.20.121.127

Primary Server Secret

\*\*\*\*\*

Test Connectivity

Secondary Server IP/Name

Secondary Server Secret

Test Connectivity

Authentication Method

☒ Default

☐ Specify

NAS IP / Called Station ID

Include in every User Group

☐

Next, go to **User & Device > User > User Groups** and create a RADIUS user group called **social\_users**.

Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Name

social\_users

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

Click to add...

Remote groups

Create NewEditDelete

| Remote Server | Group Name |
|---------------|------------|
| FAC-RADIUS    | Any        |

## 4. Configuring the FortiGate WiFi settings

Go to **WiFi & Switch Controller > WiFi Network > SSID** and select the SSID interface.

Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.

WiFi Settings

SSID

Kraven

Security Mode

Captive Portal

Portal Type

☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal

☐ Local ☒ External [https://fortiauthenticator.example.com/social\\_login/](https://fortiauthenticator.example.com/social_login/)

User Groups

social\_users

Exempt List

Click to add...

Redirect after Captive Portal

☒ Original Request ☐ Specific URL

For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social\_login/**.

For this recipe, it is set to:  
`https://fortiauthenticator.example.com/social_login/`

Set **User Groups** to the **social\_users** group.

## 5. Configuring the FortiGate to allow access to LinkedIn

On the FortiGate, configure firewall addresses to allow users to access the LinkedIn login page.

The following step can be performed in the GUI, but may take considerably longer than using the CLI. You can also copy and paste the commands below into the CLI console.

Go to **System > Dashboard** and enter the **CLI Console**. Enter the following, which creates the firewall addresses and adds them to a firewall address group called **LinkedIn\_Auth**:

```
config firewall address
  edit "www.linkedin.com"
    set type fqdn
    set fqdn "www.linkedin.com"
  next
  edit "api.linkedin.com"
    set type fqdn
    set fqdn "api.linkedin.com"
  next
  edit "static.licdn.com"
    set type fqdn
    set fqdn "static.licdn.com"
  next
  edit "help.linkedin.com"
    set type fqdn
    set fqdn "help.linkedin.com"
  next
  edit "www.fortinet.com"
    set type fqdn
    set fqdn "www.fortinet.com"
  next
end
config firewall addrgrp
  edit "LinkedIn_Auth"
    set member "api.linkedin.com" "www.linkedin.com" "help.linkedin.com"
    "www.fortinet.com" "static.licdn.com"
  next
end
```

Go to **Policy & Objects > Policy > IPv4** and create a policy for LinkedIn authentication traffic.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **LinkedIn\_Auth**.

Set **Service** to **ALL** and enable **NAT**. Configure **Security Profiles** accordingly.

|                     |                     |
|---------------------|---------------------|
| Incoming Interface  | wifi (SSID: Kraven) |
| Source Address      | all                 |
| Source User(s)      | Click to add...     |
| Source Device Type  | Click to add...     |
| Outgoing Interface  | wan1                |
| Destination Address | LinkedIn_Auth       |
| Schedule            | always              |
| Service             | ALL                 |
| Action              | ACCEPT              |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Click to add...

Go to **System > Dashboard** and enter the **CLI Console**. Add the following to exempt the LinkedIn authentication traffic policy from the captive portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

This command allows access to the external Captive Portal.

## 6. Configuring the FortiGate to allow access to FortiAuthenticator

On the FortiGate, go to **Policy & Objects > Objects > Addresses** and add the FortiAuthenticator firewall object.

For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

|                      |   |
|----------------------|---|
| Category             | <input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address |
| Name                 | FortiAuthenticator  |
| Type                 | IP/Netmask  |
| Subnet / IP Range    | 172.20.121.127  |
| Interface            | any   |
| Show in Address List | <input checked="" type="checkbox"/>   |

Go to **Policy & Objects > Policy > IPv4** and create the FortiAuthenticator access policy.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **FortiAuthenticator**.

Set **Service** to **ALL** and enable **NAT**.

|                     |                     |
|---------------------|---------------------|
| Incoming Interface  | wifi (SSID: Kraven) |
| Source Address      | all                 |
| Source User(s)      | Click to add...     |
| Source Device Type  | Click to add...     |
| Outgoing Interface  | wan1                |
| Destination Address | FortiAuthenticator  |
| Schedule            | always              |
| Service             | ALL                 |
| Action              | ACCEPT              |

Firewall / Network Options

ON NAT

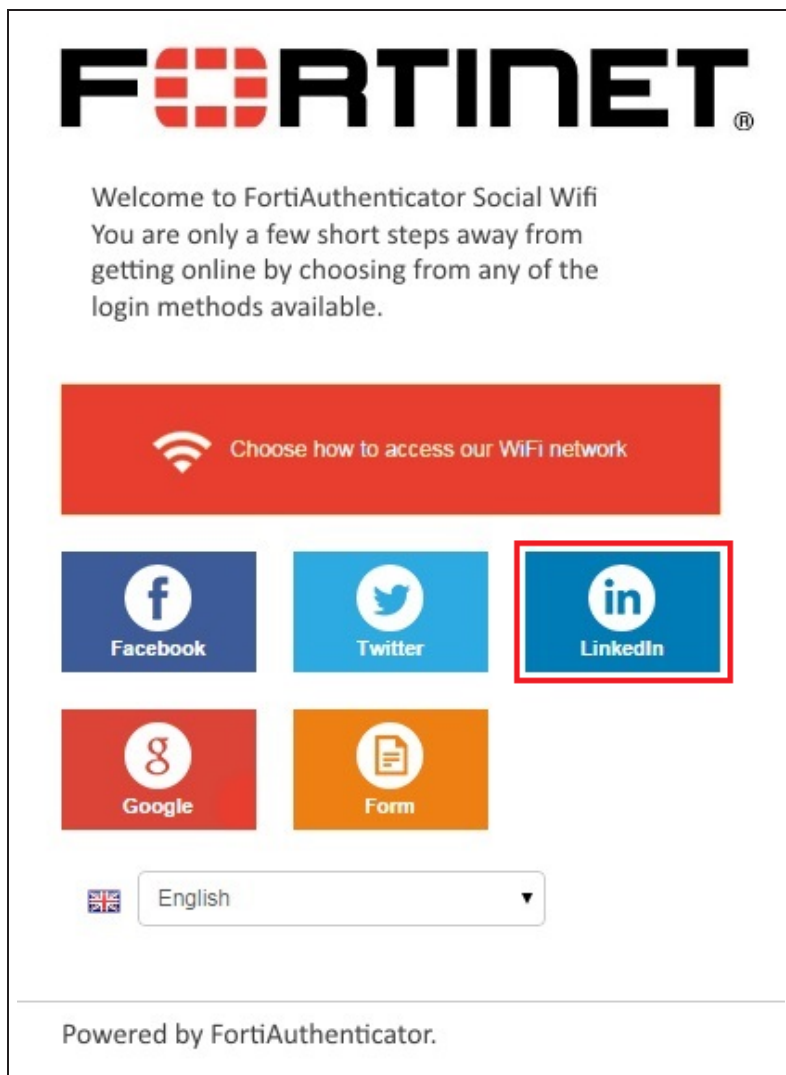
Add the following to exempt the FortiAuthenticator access policy from the Captive Portal:

```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

## 7. Results

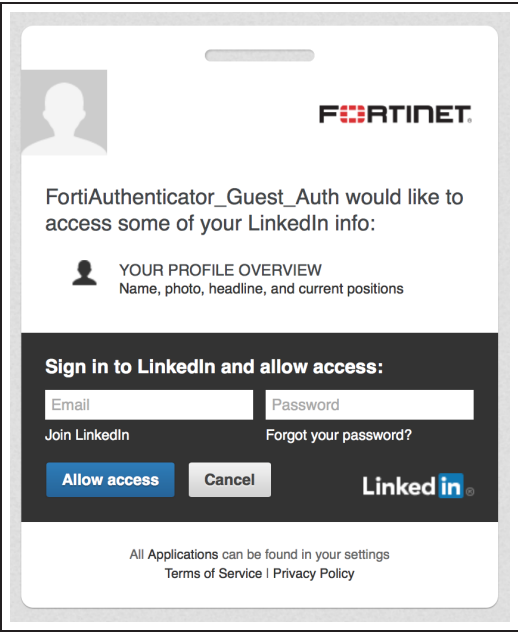
Connect to the WiFi and attempt to browse the Internet. You will be redirected to the Captive Portal splash page.

Select **LinkedIn** and you should be redirected to the LinkedIn login page.






Enter valid LinkedIn credentials and you will be redirected to the URL initially requested.

You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.



To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

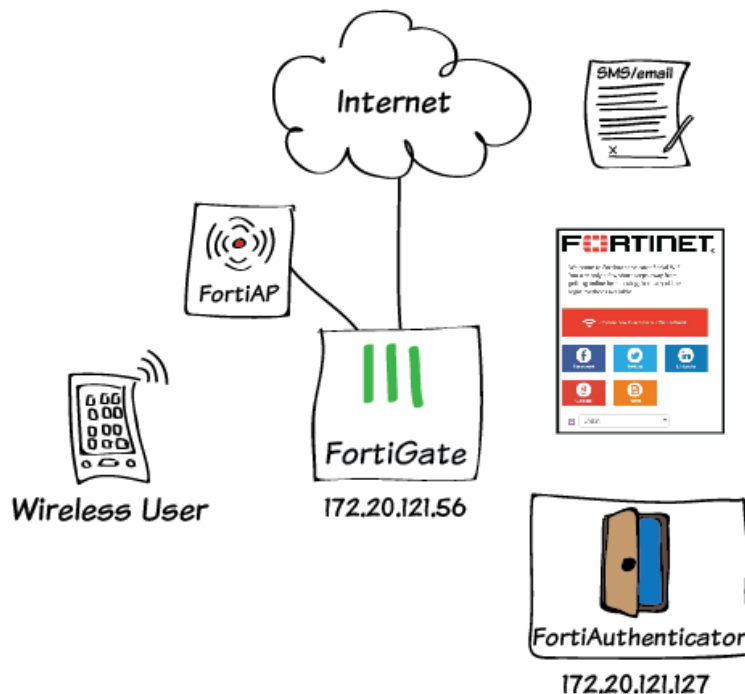
| <div><div> Delete</div><div>0 of 1 selected</div></div> |                |                     |            |           |               |   | <div><div>Search for social login users</div><div></div></div> |              |                         |
|--|----------------|---------------------|------------|-----------|---------------|---|---|--------------|-------------------------|
| <input type="checkbox"/>   | Login id       | User                | First name | Last name | Email address | Active  | Mac address   | Groups       | Expiration              |
| <input type="checkbox"/>   | SocialLogin_34 | linkedin:WadeWilson | Wade       | Wilson    |               |  | 3c:15:c2:e3:3c:22   | Social_Users | Fri Sep 4 18:47:54 2015 |
| 1 social login user  |                |                     |            |           |               |   |   |              |                         |

You can configure Captive Portal to use other social WiFi logins:

- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (Form-based)



# Social WiFi Captive Portal with FortiAuthenticator (Form-based)



WiFi authentication using a forms-based portal provides access control without having to manually create guest accounts.

This recipe involves setting up a social portal RADIUS service on the FortiAuthenticator, and configuring the FortiGate for Captive Portal access, allowing users to log in to the WiFi network using either SMS or e-mail self-registration.

This recipe is similar to the [Captive portal WiFi access control](#) recipe, but involves RADIUS authentication, and does not include FortiAP registration instructions.

# 1. Configuring the social portal RADIUS service on FortiAuthenticator

Go to **Authentication > User Management > User Groups**, and create a **Social\_Users** user group.

Users that log in through the forms-based authentication method will be placed in this group once it is added to the Captive Portal General Settings.

Name: **Social\_Users**

Type: ☒ Local ☐ Remote LDAP ☐ Remote RADIUS

Users:

Available users: Filter

Selected users:

Choose all visible Remove all

| Attribute                     | Value | Vendor | Actions |
|-------------------------------|-------|--------|---------|
| <a href="#">Add Attribute</a> |       |        |         |

OK Cancel

Go to **Authentication > RADIUS Service > Clients**, and create a new RADIUS client.

Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, 172.20.121.56).

Enable the **Social portal** captive portal.

Name: RADIUSclient

Client name/IP: 172.20.121.56

Secret: \*\*\*\*\*

Enable captive portal:

☐ Credential portal (URL: /captive\_login)

☒ Social portal (URL: /social\_login)

☐ MAC address portal (URL: /mac\_login)

| Profile name | Description | Authentication method  | Username input format   | Realms              | Allow local users to override remote users | Use Windows AD domain authentication | Groups   | Delete |
|--------------|-------------|--|---|---------------------|--|--------------------------------------|--|--------|
| Default      |             | <input type="radio"/> Enforce two-factor authentication<br><input type="radio"/> Apply two-factor authentication if available (authenticate any user)<br><input checked="" type="radio"/> Password-only authentication (exclude users without a password)<br><input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken) | <input checked="" type="radio"/> username@realm<br><input type="radio"/> realmusername<br><input type="radio"/> realmusername | local   Local users | <input type="checkbox"/>                   | <input type="checkbox"/>             | <input checked="" type="checkbox"/> Filter: Social_Users (local)<br><input type="checkbox"/> Filter: local users (all) |        |

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Allow MAC-based authentication

Check machine authentication

EAP types:

☐ EAP-GTC  
☐ EAP-TLS  
☐ PEAP  
☐ EAP-TTLS

Save

OK Cancel

Enter the pre-shared **Secret** and set the **Authentication method**. The FortiGate will use this secret key in its RADIUS configuration.

Add the **Social\_Users** user group to the **Realms** group filter as shown.

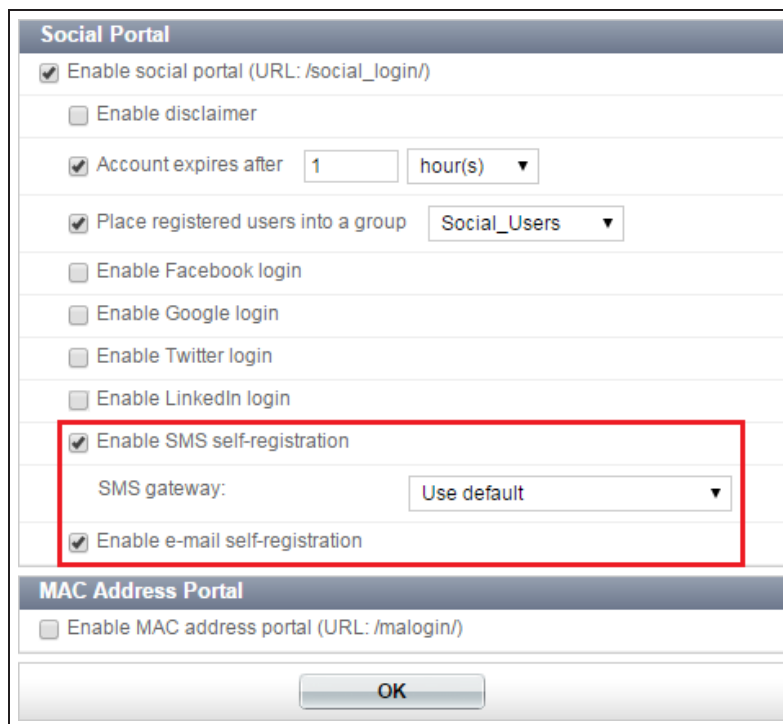
Select **Save** and then **OK**.

Next go to **Authentication > Captive Portal > General** and enable **Social Portal**.

Configure the account expiry time (in the example it is set to 1 hour).

Set **Place registered users into a group** to **Social\_Users**.

Enable the **SMS self-registration** and **e-mail self-registration** login options. Be sure **SMS gateway** is set to **Use default**.



**Social Portal**

- ☒ Enable social portal (URL: /social\_login/)
- ☐ Enable disclaimer
- ☒ Account expires after  hour(s) ▼
- ☒ Place registered users into a group  ▼
- ☐ Enable Facebook login
- ☐ Enable Google login
- ☐ Enable Twitter login
- ☐ Enable LinkedIn login
- ☒ Enable SMS self-registration
  - SMS gateway:  ▼
- ☒ Enable e-mail self-registration

**MAC Address Portal**

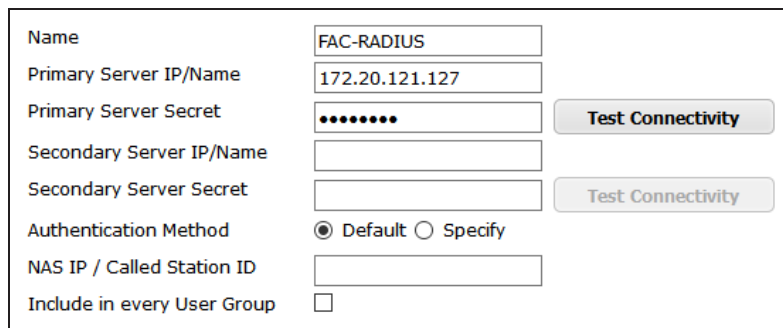
- ☐ Enable MAC address portal (URL: /malogin/)

OK

## 2. Configuring the FortiGate authentication settings

On the FortiGate, go to **User & Device > Authentication > RADIUS Servers** and create the connection to the FortiAuthenticator RADIUS server, using its IP and pre-shared secret.

Use the **Test Connectivity** option with valid credentials to test the connection.



Name:

Primary Server IP/Name:

Primary Server Secret:

Secondary Server IP/Name:

Secondary Server Secret:

Authentication Method: ☒ Default ☐ Specify

NAS IP / Called Station ID:

Include in every User Group: ☐

Next, go to **User & Device > User > User Groups** and create a RADIUS user group called **social\_users**.

Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.

Name

social\_users

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members

Click to add...

Remote groups

Create New

Edit

Delete

| Remote Server | Group Name |
|---------------|------------|
| FAC-RADIUS    | Any        |

### 3. Configuring the FortiGate WiFi settings

Go to **WiFi & Switch Controller > WiFi Network > SSID** and select the SSID interface.

Under **WiFi Settings**, set the **Security Mode** to **Captive Portal**.

WiFi Settings

SSID

Kraven

Security Mode

Captive Portal

Portal Type

☒ Authentication ☐ Disclaimer + Authentication ☐ Disclaimer Only ☐ Email Collection

Authentication Portal

☐ Local ☒ External 

https://fortiauthenticator.example.com/social\_login/

User Groups

social\_users

Exempt List

Click to add...

Redirect after Captive Portal

☒ Original Request ☐ Specific URL

For the **Authentication Portal**, select **External**, and enter the FQDN of the FortiAuthenticator, followed by **/social\_login/**.

For this recipe, it is set to:  
`https://fortiauthenticator.example.com/social_login/`

Set **User Groups** to the **social\_users** group.

### 4. Configuring the FortiGate to allow access to FortiAuthenticator

On the FortiGate, go to **Policy & Objects > Objects > Addresses** and add the FortiAuthenticator firewall object.

For **Subnet/IP Range** enter the IP address of the FortiAuthenticator.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FortiAuthenticator

Type

IP/Netmask

Subnet / IP Range

172.20.121.127

Interface

any

Show in Address List

☒

Go to **Policy & Objects > Policy > IPv4** and create the FortiAuthenticator access policy.

Set **Incoming Interface** to the WiFi SSID interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **FortiAuthenticator**.

Set **Service** to **ALL** and enable **NAT**.

|  |                     |
|--|---------------------|
| Incoming Interface                         | wifi (SSID: Kraven) |
| Source Address                             | all                 |
| Source User(s)                             | Click to add...     |
| Source Device Type                         | Click to add...     |
| Outgoing Interface                         | wan1                |
| Destination Address                        | FortiAuthenticator  |
| Schedule                                   | always              |
| Service                                    | ALL                 |
| Action                                     | ACCEPT              |
| <b>Firewall / Network Options</b>          |                     |
| <input checked="" type="checkbox"/> ON NAT |                     |

Add the following to exempt the FortiAuthenticator access policy from the Captive Portal:

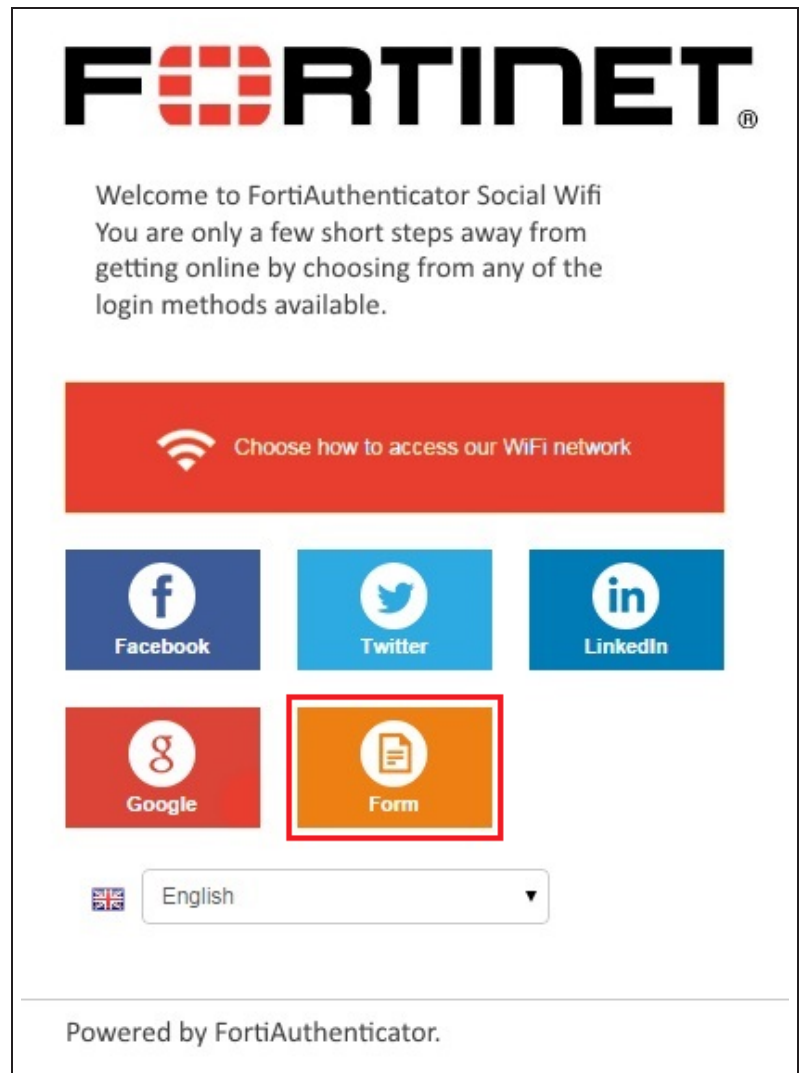
```
config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  next
end
```

This command allows access to the external Captive Portal.

## 5. Results

Connect to the WiFi and attempt to browse the Internet. You will be redirected to the Captive Portal splash page.

Select **Form-based** and you should be redirected to the Form-based authentication login page.



Select your preferred **Verification method**, enter valid credentials, and select **Submit**. You will be redirected to the URL initially requested.

You can now browse freely until the social login account expires, as configured on the FortiAuthenticator under **Authentication > Captive Portal > General**.

To view the authenticated user added on FortiAuthenticator, go to **Authentication > User Management > Social Login Users**.

Please enter your information below.

**First name:**

**Last name:**

**Verification method:**

☒ E-mail ☐ SMS

**Email address:**

Submit

Cancel

| Delete                   | 0 of 1 selected |                        | Search for social login users |           |                   |        |                   |              |                         |
|--------------------------|-----------------|------------------------|-------------------------------|-----------|-------------------|--------|-------------------|--------------|-------------------------|
|                          | Login id        | User                   | First name                    | Last name | Email address     | Active | Mac address       | Groups       | Expiration              |
| <input type="checkbox"/> | SocialLogin_36  | email.wilson.fortinet@ | Wilde                         | Wilson    | wwilson.fortinet@ |        | 3c:15:c2:e3:3c:22 | Social_Users | Fri Sep 4 19:20:54 2015 |
| 1 social login user      |                 |                        |                               |           |                   |        |                   |              |                         |

You can configure Captive Portal to use other social WiFi logins:

- Social WiFi Captive Portal with FortiAuthenticator (Facebook)
- Social WiFi Captive Portal with FortiAuthenticator (Twitter)
- Social WiFi Captive Portal with FortiAuthenticator (Google+)
- Social WiFi Captive Portal with FortiAuthenticator (LinkedIn)

# Expert

FortiGate units can be deployed in many ways to meet a wide range of advanced requirements. This section contains recipes and articles (which discuss topics in greater depth than a recipe) about a variety of these configurations.

Recipes and articles in this section are intended for users with a high degree of background knowledge about FortiGates and computer networking, such as users who have completed Fortinet's **Network Security Expert (NSE) 4** level of training.

## High Availability

- [High Availability with FGCP](#)
- [Redundant architecture](#)
- [SLBC setup with one FortiController-5103B](#)
- [SLBC Active-Passive setup with two FortiController-5103Bs](#)
- [SLBC Active-Passive with two FortiController-5103Bs and two chassis](#)
- [SLBC Dual Mode with two FortiController-5103Bs](#)
- [SLBC Active-Passive with four FortiController-5103Bs and two chassis](#)
- [SLBC Dual Mode with two FortiController-5903Cs](#)

## IPsec VPN

- [BGP over a dynamic IPsec VPN](#)
- [OSPF over dynamic IPsec VPN](#)

## Authentication

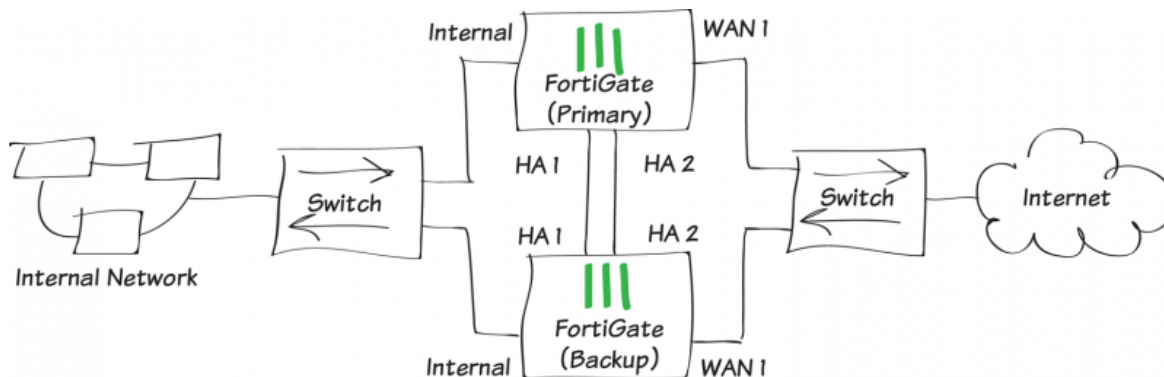
- [Single Sign-on using LDAP and FSSO agent in advanced mode](#)
- [Single Sign-On using FSSO agent in advanced mode and FortiAuthenticator](#)
- [SSO using a FortiGate, FortiAuthenticator, and DC Polling](#)

## Articles

- [Hub-and-spoke VPN using quick mode selectors](#)



# High Availability with FGCP



This recipe describes how to enhance the reliability of a network protected by a FortiGate unit by adding a second FortiGate unit and setting up a FortiGate Clustering Protocol (FGCP) High Availability cluster.

The FortiGate already on the network will be configured to become the primary unit by increasing its device priority and enabling override. The new FortiGate will be prepared by setting it to factory defaults to wipe any configuration changes. Then it will be licensed, configured for HA, and then connected to the FortiGate already on the network. The new FortiGate becomes the backup unit and its configuration is overwritten by the primary unit.

The recipe contains instructions for both the GUI and the CLI, with some parts of the configuration requiring use of the CLI. For a simplified HA recipe that only requires use of the GUI, see [High Availability with two FortiGates](#).

Before you start the FortiGates should be running the same FortiOS firmware version and interfaces should not be configured to get their addresses from DHCP or PPPoE.

# 1. Configuring the primary FortiGate

If the FortiGates in the cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Connect to the primary FortiGate and go to **System > Dashboard > Status** and locate the **System Information** widget.

Change the unit's **Host Name** to identify it as the primary FortiGate.

You can also enter this CLI command:

```
Current Name FG100D3G12804410
New Name Primary_FortiGate
```

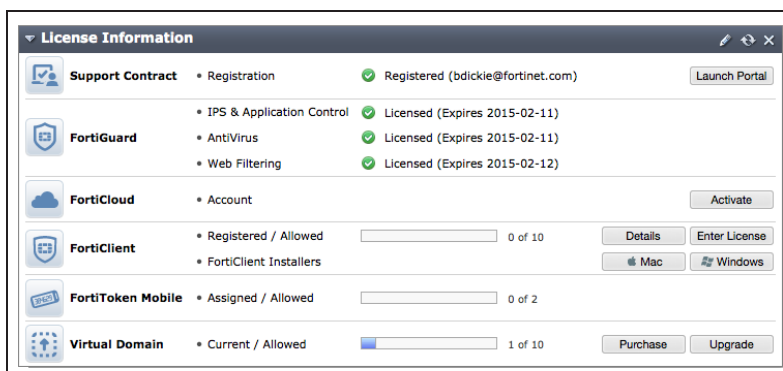
```
config system global
set hostname Primary_FortiGate
end
```

If you have not already done so, register the primary FortiGate and apply licenses to it before setting up the cluster. This includes **FortiCloud** activation, **FortiClient** and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed third-party certificates are synchronized to the backup FortiGate.

Enter this CLI command to set the HA mode to active-passive, set a group name and password, increase the device priority to a higher value (for example, 250) and enable override.

Enabling override and increasing the device priority means this unit should always become the primary unit.

This command also selects ha1 and ha2 to be the heartbeat interfaces and sets



```
config system ha
set mode a-p
set group-name My-HA-Cluster
set password
set priority 250
set override enable
set hbdev ha1 50 ha2 50
end
```

their priorities to 50.

You can also use the GUI to configure most of these settings.

Mode

Active-Passive

Device Priority

250

☐ Reserve Management Port for Cluster Member

Internal

Cluster Settings

Group Name

My-HA-Cluster

Password

\*\*\*\*\*

☐ Enable Session Pick-up

|                          | Port Monitor             | Heartbeat Interface                 |                 |
|--------------------------|--------------------------|-------------------------------------|-----------------|
|                          |                          | Enable                              | Priority(0-512) |
| dmz (DMZ server network) | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| ha1                      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 50              |
| ha2                      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 50              |
| mgmt                     | <input type="checkbox"/> |                                     |                 |
| port9                    | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| port10                   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| port11                   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| port14                   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| port15                   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| port16                   | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| wan1                     | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |
| wan2                     | <input type="checkbox"/> | <input type="checkbox"/>            | 0               |

Override can only be enabled from the CLI.

```
config system ha
set override enable
end
```

The FortiGate unit negotiates to establish an HA cluster. When you select OK you may temporarily lose connectivity with the FortiGate unit as FGCP negotiation takes place and the MAC addresses of the FortiGate unit are changed to HA virtual MAC addresses. These virtual MAC addresses are used for failover. The actual virtual MAC address assigned to each FortiGate interface depends on the HA group ID. Since this example does not involved changing the HA group ID, the FortiGate unit's interfaces will have the following MAC

addresses: 00:09:0f:09:00:00, 00:09:0f:09:00:01, 00:09:0f:09:00:02 and so on.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all arp table entries). You can usually delete the arp table from a command prompt using a command similar to `arp -d`.

To confirm these MAC address changes, you can use the `get hardware nic` (or `diagnose hardware deviceinfo nic`) command to view the virtual MAC address of any FortiGate unit interface. Depending on the FortiGate model, the output from this command could include lines similar to the following:

```
Current_HWaddr: 00:09:0f:09:00:00
Permanent_HWaddr 02:09:0f:78:18:c9
```

## 2. Configuring the backup FortiGate

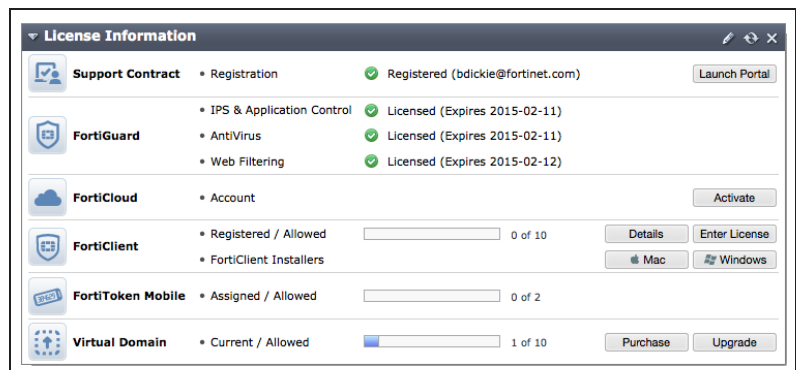
Enter this command to reset the new FortiGate to factory default settings.

```
execute factoryreset
```

You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all it is recommended to set it back to factory defaults to reduce the chance of synchronization problems.

Change the firmware running on the new FortiGate to be the same version as is running on the primary unit.

Register the backup FortiGate and apply licenses to it before setting up the cluster. This includes **FortiCloud** activation, **FortiClient** and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs).



Go to **System > Dashboard > Status** and change the unit's **Host Name** to identify it as the backup FortiGate.

|                     |   |
|---------------------|---|
| <b>Current Name</b> | FG100D3G12801361                              |
| <b>New Name</b>     | <input type="text" value="Backup_FortiGate"/> |

You can also enter this CLI command:

```
config system global
set hostname Backup_FortiGate
end
```

Duplicate the primary unit HA settings, except set the device priority to a lower value and do not enable override.

You can configure all of these settings from the GUI.

Mode

Active-Passive

Device Priority

50

☐ Reserve Management Port for Cluster Member

Internal

Cluster Settings

Group Name

My-HA-Cluster

Password

.....

☐ Enable Session Pick-up

|                          | Port Monitor             | Heartbeat Interface                 |                 |
|--------------------------|--------------------------|-------------------------------------|-----------------|
|                          |                          | Enable                              | Priority(0-512) |
| dmz (DMZ server network) | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| ha1                      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <div>50</div>   |
| ha2                      | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <div>50</div>   |
| mgmt                     | <input type="checkbox"/> |                                     |                 |
| port9                    | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port10                   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port11                   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port14                   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port15                   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| port16                   | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| wan1                     | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |
| wan2                     | <input type="checkbox"/> | <input type="checkbox"/>            | <div>0</div>    |

You can also enter this CLI command:

```
config system ha
set mode a-p
set group-name My-HA-Cluster
set password
set priority 50
set hbdev ha1 50 ha2 50
end
```

### 3. Connecting the cluster

Connect the HA cluster as shown in the initial diagram. Making these connections will disrupt network traffic as you disconnect and re-connect cables.

When connected the primary and backup FortiGates find each other and negotiate to form an HA cluster. The Primary unit synchronizes its configuration with the backup FortiGate. Forming the cluster happens automatically with minimal or no disruption to network traffic.

### 4. Checking cluster operation and disabling override

Check the cluster synchronization status to make sure the primary and backup units have the same configuration. Log into the primary unit CLI and enter this command:

```
diag sys ha cluster-csum
```

The command output lists all members' checksums. If both cluster units have identical checksums you can be sure that their configurations are synchronized. If the checksums are different wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical contact Fortinet support to help troubleshoot the problem.




When the checksums are identical, disable override on the primary unit (recommended).

```
config system ha
  set override disable
end
```



The HA cluster dynamically responds to network conditions. If you keep override enabled the same FortiGate will always be the primary FortiGate. Because of this, however; the cluster may negotiate more often potentially disrupting traffic.

If you disable override it is more likely that the new FortiGate unit could become the primary unit. Disabling override is recommended unless its important that the same FortiGate remains the primary unit.

Connect to the primary FortiGate GUI and go to **System > Config > HA** to view the cluster information.

| Cluster Member  |   | Hostname          | Serial No.       | Role   | Priority |
|---|---|-------------------|------------------|--------|----------|
|  |  | Primary_FortiGate | FG100D3G12804410 | MASTER | 128      |
|   |  | Backup_FortiGate  | FG100D3G12801361 | SLAVE  | 50       |

Select **View HA Statistics** for more information on how the cluster is operating and processing traffic.

| Unit                                  | Status  | Up Time    | Monitor      |                     |               |
|---------------------------------------|---|------------|--------------|---------------------|---------------|
| Primary_FortiGate<br>FG100D3G12804410 |  | 0 days     | CPU Usage    | Active Sessions     | Total Packets |
|                                       |   | 1 hours    | 1%           | 26                  | 81857         |
|                                       |   | 44 minutes | Memory Usage | Network Utilization | Total Bytes   |
|                                       |   | 2 seconds  | 34%          | 78 Kbps             | 27300058      |
| Backup_FortiGate<br>FG100D3G12801361  |  | 2 days     | CPU Usage    | Active Sessions     | Total Packets |
|                                       |   | 0 hours    | 0%           | 6                   | 8718576       |
|                                       |   | 15 minutes | Memory Usage | Network Utilization | Total Bytes   |
|                                       |   | 15 seconds | 19%          | 13 Kbps             | 2778691497    |

## 5. Results

Normally, traffic should now be flowing through the primary FortiGate. However, if the primary FortiGate is unavailable, traffic should failover and the backup FortiGate will be used. Failover will also cause the primary and backup FortiGates to reverse roles, even when both FortiGates are available again.

To test this, ping the IP address 8.8.8.8 using a PC on the internal network. After a moment, power off the primary FortiGate.

*If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.*

You will see a momentary pause in the Ping results, until traffic diverts to the backup FortiGate, allowing the Ping

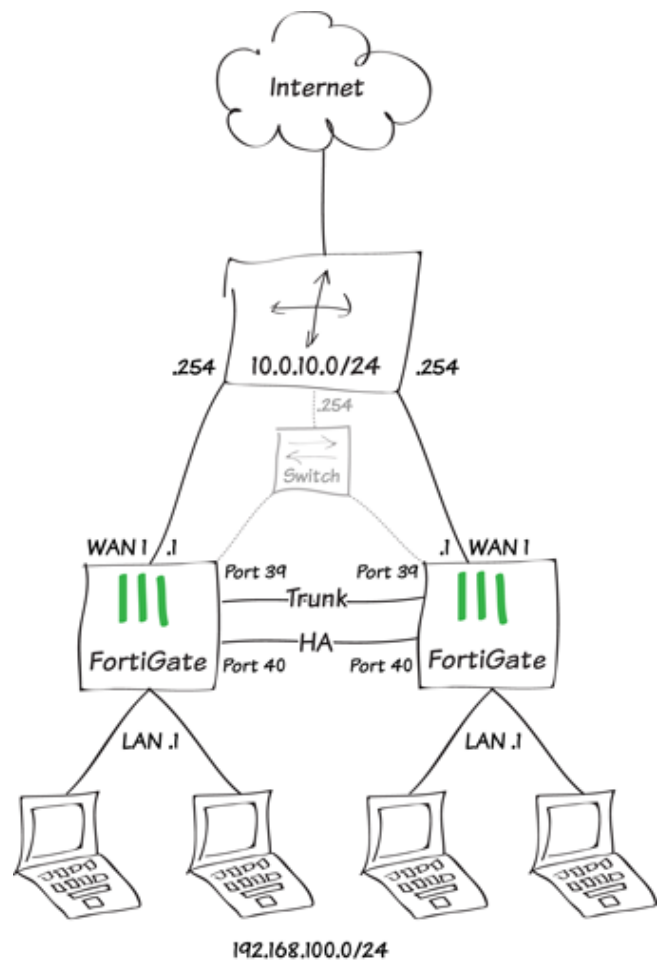
```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

traffic to continue.

For further reading, check out [Configuring and connecting HA clusters](#) in the [FortiOS 5.2 Handbook](#).



# Redundant architecture



The following recipe provides useful instructions for customers with multi-site architecture and redundant firewalls. It is intended for those customers that want to reduce the number of on-site appliances while increasing network security and decreasing Total Cost of Ownership, where the goal is simple, cost-effective reliability.

FortiOS 5.2 introduced many new features that we will use in this configuration, which is therefore not possible on FortiOS 5.0.x or earlier. The recipe is performed with the FortiGate 1xxD/2xxD series.

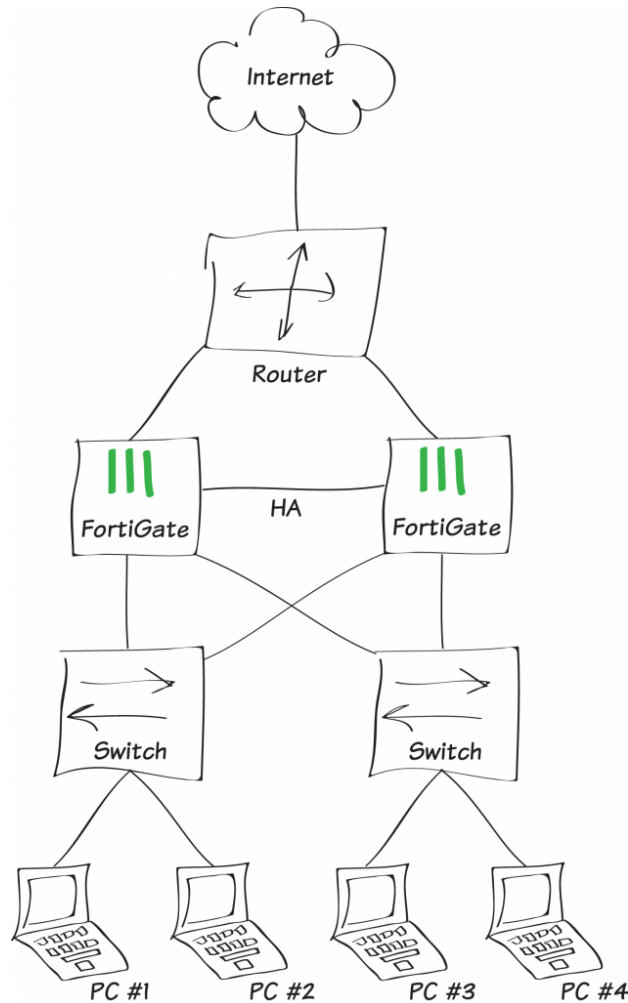
By following the recipe, you will be able to provide your small-site customers with simple, yet secure infrastructure that perfectly matches the UTM approach, where we want to centralize as many security features as possible on a single device or cluster.

The recipe provides task-oriented instructions for administrators to fully complete the installation. It is divided into the following sections:

1. **Scenario**: This section explains the problems that this new network topology solves, including the cases in which the topology should be used.
2. **Topology**: This section includes diagrams of the new topology. It also lists key advantages to this kind of architecture and explains why it solves the problems previously identified in The Scenario.
3. **Configuration**: This section provides step-by-step instructions for configuring the FortiGates within the new topology.

# Scenario

In the standard scenario, we assume the following topology as the starting point:



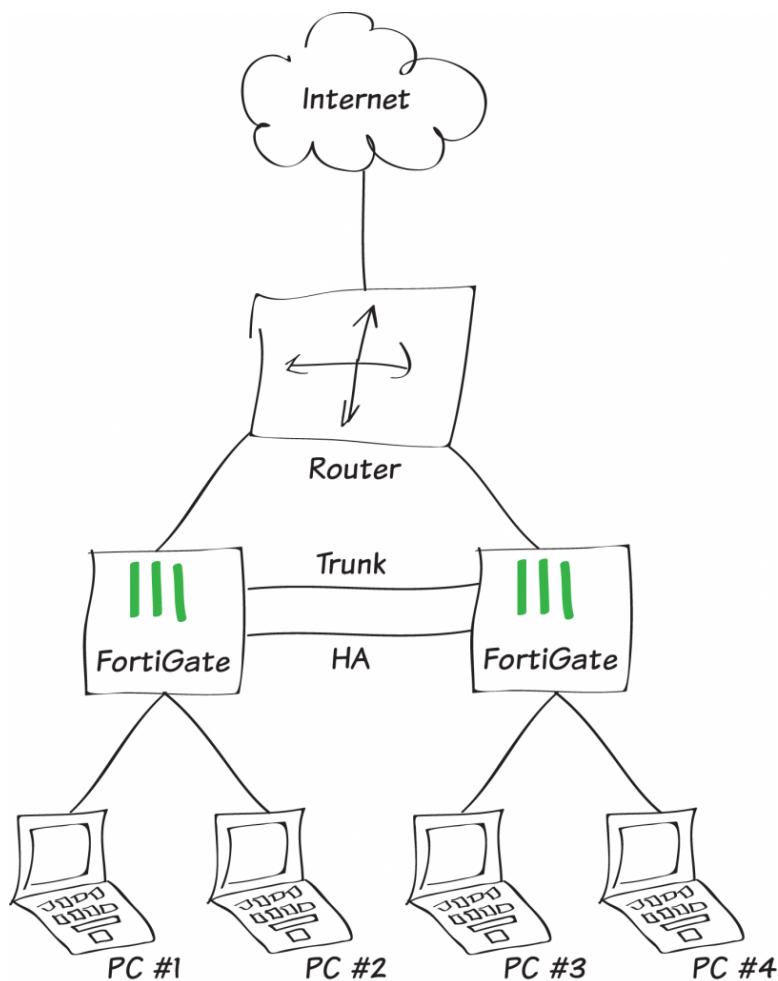
Multi-site customers that want to avoid any “Single Point of Failure” in their remote networks often use this kind of topology. These customers require two FortiGates in Active/Passive mode and therefore two switches on the LAN side to transfer Ethernet payloads to the active FortiGate. There are a few downsides to this approach:

- Four appliances need to be managed and supervised.
- Administrators must know how to work with the Firewall OS and with the Switch OS.
- If one switch fails, the workstations connected won't be able to reach the Internet.
- Most of the firewall ports are not used.

# Topology

In this section, we look at the target topology and the scenarios for FortiGate failover. At the end of the section, we discuss the key advantages of adopting the target topology.

## 2.1 The Target Topology



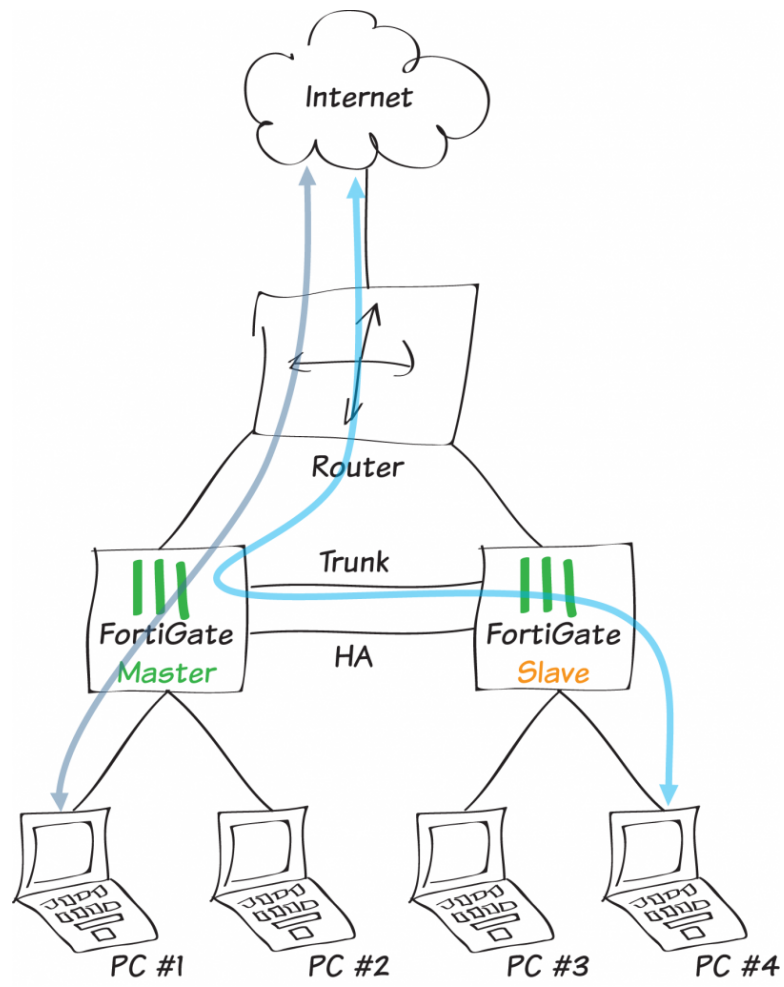
In this new topology, we won't be using additional switches. Instead, we will be using the FortiGate's Integrated Switch Fabric (ISF) solution on both master and slave firewalls.

Note that the target topology uses a FortiGate 2xxD, which has 40 ports. In your configuration, ensure that each FortiGate has enough ports to handle all of the computers in the event of a failover, or switches will still need to be involved.

The administrator will have to configure a trunk link between the two FortiGate physical switches to expand subnets and VLANs from one firewall to the other.

In a FortiGate cluster using FGCP, the slave firewall's ISF can still be used to send traffic destined for the active member across the trunk link.

A representation of the traffic flow appears below:

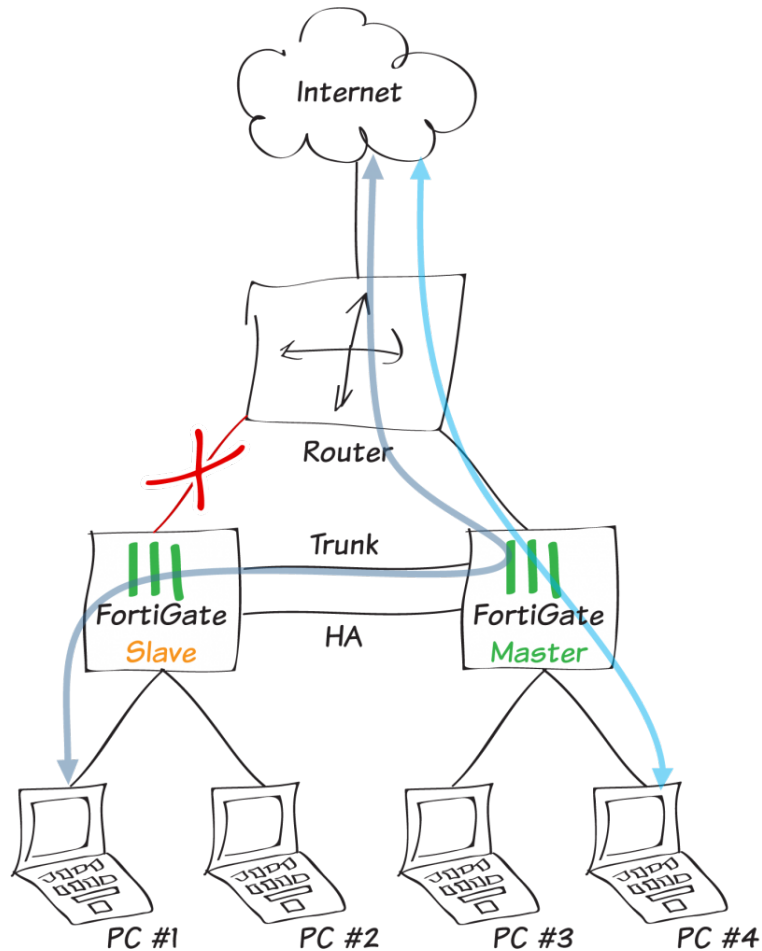


## 2.2 FortiGate Failover

### Case 1: Link failure

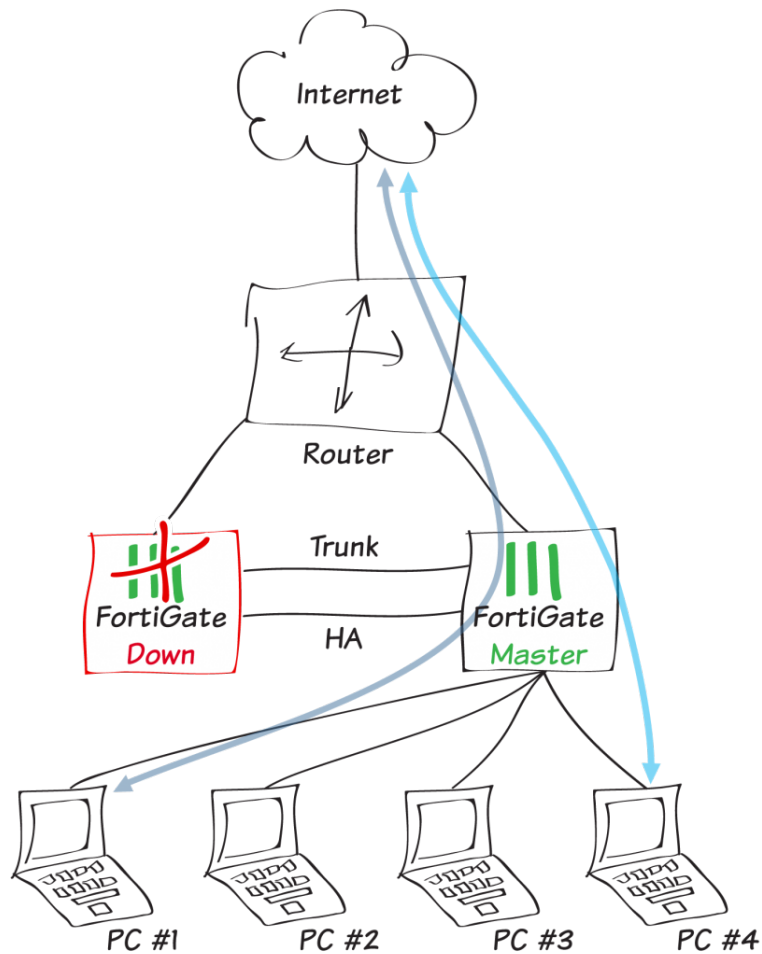
The diagram below represents traffic flow in the event of a failover in the following cases:

- The monitored WAN port, on what was originally the Master FortiGate, fails.
- The link between the router and the original Master FortiGate fails.



## Case 2: FortiGate global failure

If the master were to completely fail (including the ISF), the administrator would have to plug the LAN segments into the remaining firewall, just as if one switch were to fail in our standard topology.



## 2.3 Key Advantages

This new topology offers a few key advantages:

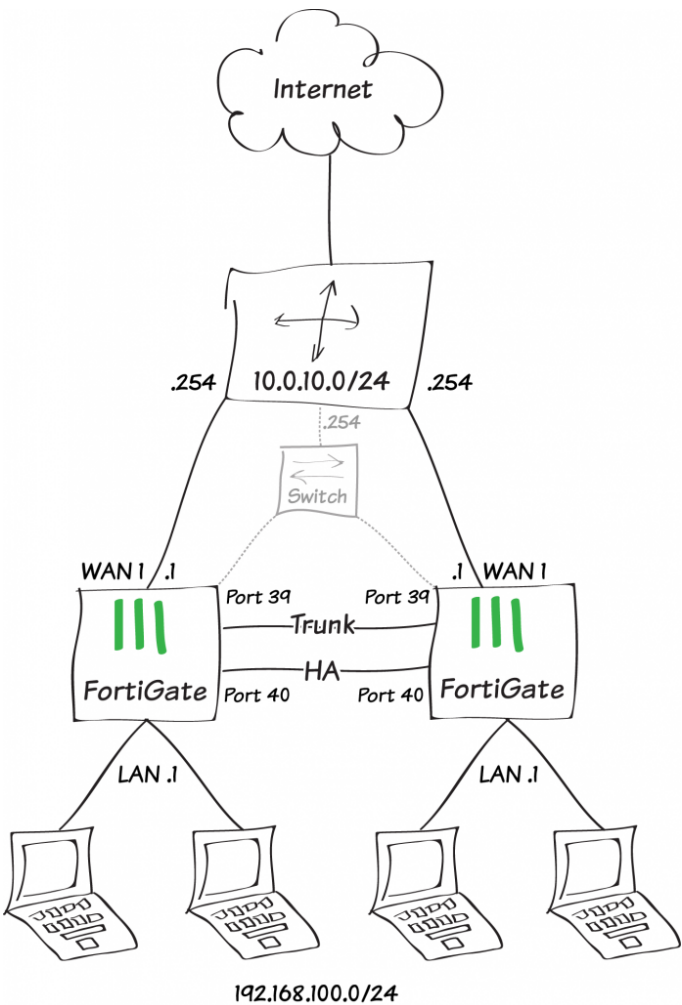
- Only two devices are required, where four are required in the standard topology.
- It is easier for the administrator to manage security and switching on a single device.
- The use of FortiManager simplifies central management.
- There is only one cluster to supervise.

# Configuration

In this section, we reproduce the following network topology. Notice how the router has a switch interface. If your router does not have a switch interface, you will have to add an extra switch (noted in gray below), and in the event of a firewall crash, you will have to power cycle the router.

As we will be changing the configuration of the hardware switch, we strongly recommend that you use the management port to follow the steps below.

By default, the FortiGate management IP address is 192.168.1.99/24.





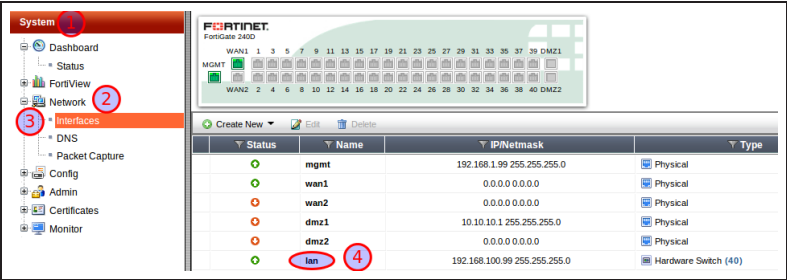
# 1. Configuring the hardware switch

By default on a FortiGate 1xxD/2xxD, the unit is in Interface mode and all of the internal ports are attached to a hardware switch named **lan**. In this example, we need to use ports 39 and 40 for Trunk and HA respectively.

The first step is to remove ports 39 and 40 from the Hardware Switch lan. Begin by editing the lan interface.

*If the unit is in Switch mode, it will have to be reconfigured into Interface mode. For more information, see [Choosing your FortiGate's switch mode](#).*

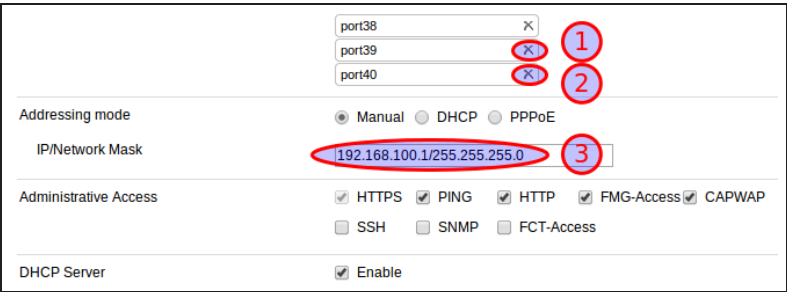
Go to **System > Network > Interfaces** and double-click **lan** in the interface list.



Remove the last two ports in the list, in this case **port39** and **port40**.

Then configure the **IP/Network Mask** with the following address:  
*192.168.100.1/255.255.255.0*

When you are done, accept the change.



The interface list should now look like this:

| Status | Name   | IP/Netmask                  | Type                 |
|--------|--------|-----------------------------|----------------------|
| Up     | mgmt   | 192.168.1.99 255.255.255.0  | Physical             |
| Up     | wan1   | 0.0.0.0 0.0.0.0             | Physical             |
| Down   | wan2   | 0.0.0.0 0.0.0.0             | Physical             |
| Down   | dmz1   | 10.10.10.1 255.255.255.0    | Physical             |
| Down   | dmz2   | 0.0.0.0 0.0.0.0             | Physical             |
| Up     | lan    | 192.168.100.1 255.255.255.0 | Hardware Switch (38) |
| Down   | port39 | 0.0.0.0 0.0.0.0             | Physical             |
| Down   | port40 | 0.0.0.0 0.0.0.0             | Physical             |

For the trunk port to work properly, we need to configure a vlan ID on the Virtual Switch. This can only be done in the CLI.

```
FGT1 # config system global
FGT1 (global) # set virtual-switch-vlan enable
FGT1 (global) # end
FGT1 # show system global
```

First we need to enable this feature globally. Use the commands shown here:

```
config system global
  set fgd-alert-subscription advisory latest-threat
  set hostname "FGT1"
  set internal-switch-mode interface
  set optimize antivirus
  set timezone 04
  set virtual-switch-vlan enable
end
```

Next, edit the Virtual Switch and set the vlan number:

```
FGT1 # config system virtual-switch
FGT1 (virtual-switch) # edit lan
FGT1 (lan) # set vlan 100
FGT1 (lan) # end
```

You should now be able to see VLAN Switch in the interface list.

| Status | Name               | IP/Netmask                  | Type             |
|--------|--------------------|-----------------------------|------------------|
| ✔      | mgmt               | 192.168.1.99 255.255.255.0  | Physical         |
| ✔      | wan1               | 0.0.0.0 0.0.0.0             | Physical         |
| ✖      | wan2               | 0.0.0.0 0.0.0.0             | Physical         |
| ✖      | dmz1               | 10.10.10.1 255.255.255.0    | Physical         |
| ✖      | dmz2               | 0.0.0.0 0.0.0.0             | Physical         |
| ✔      | lan (VLAN ID: 100) | 192.168.100.1 255.255.255.0 | VLAN Switch (38) |
| ✖      | port39             | 0.0.0.0 0.0.0.0             | Physical         |
| ✖      | port40             | 0.0.0.0 0.0.0.0             | Physical         |

## 2. Configuring the trunk port

The trunk port will be used to allow traffic to flow between the Virtual Switch of each FortiGate.

Configuring the trunk port is only possible in the CLI:

```
FGT1 # config system interface
FGT1 (interface) # edit port39
FGT1 (port39) # set trunk enable
FGT1 (port39) # end
FGT1 # show system interface port39
config system interface
  edit "port39"
    set [glossary_exclude]vdom[/glossary_exclude] "root"
    set type physical
    set trunk enable
    set [glossary_exclude]snmp[/glossary_exclude]-index 10
  next
end
```

You should now be able to see the trunk port in the interface list.

| Status | Name               | IP/Netmask                  | Type             |
|--------|--------------------|-----------------------------|------------------|
| ✔      | mgmt               | 192.168.1.99 255.255.255.0  | Physical         |
| ✔      | wan1               | 0.0.0.0 0.0.0.0             | Physical         |
| ✖      | wan2               | 0.0.0.0 0.0.0.0             | Physical         |
| ✖      | dmz1               | 10.10.10.1 255.255.255.0    | Physical         |
| ✖      | dmz2               | 0.0.0.0 0.0.0.0             | Physical         |
| ✔      | lan (VLAN ID: 100) | 192.168.100.1 255.255.255.0 | VLAN Switch (38) |
| ✖      | port39             | Dedicate as Ethernet Trunk  | Physical         |
| ✖      | port40             | 0.0.0.0 0.0.0.0             | Physical         |

### 3. Configuring HA

We will now configure High Availability. Port 40 will be used for HeartBeat/Sync communications between cluster members. Port Wan1 will be monitored.

Go to **System > Config > HA** and configure High Availability as shown:

Mode

Active-Passive

Device Priority

128

☐ Reserve Management Port for Cluster Member

dmz1

Cluster Settings

Group Name

fgt

Password

.....

☒ Enable Session Pick-up

|        | Port Monitor                        | Heartbeat Interface                 |                 |
|--------|-------------------------------------|-------------------------------------|-----------------|
|        |                                     | Enable                              | Priority(0-512) |
| dmz1   | <input type="checkbox"/>            | <input type="checkbox"/>            | <div>0</div>    |
| dmz2   | <input type="checkbox"/>            | <input type="checkbox"/>            | <div>0</div>    |
| mgmt   | <input type="checkbox"/>            |                                     |                 |
| port39 | <input type="checkbox"/>            | <input type="checkbox"/>            | <div>0</div>    |
| port40 | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <div>0</div>    |
| wan1   | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <div>50</div>   |
| wan2   | <input type="checkbox"/>            | <input type="checkbox"/>            | <div>50</div>   |

#### 4. Configuring WAN1 IP routing

Go to **System > Network > Interfaces** and edit **wan1** as shown.

Interface Name

wan1(08:5B:0E:32:5C:E4)

Alias

1Internet

Link Status

Up

Type

Physical Interface

Addressing mode

2Manual ☐ DHCP ☐ PPPoE ☐ Dedicate to Extension Device ☐

IP/Network Mask

310.0.10.1/24

Administrative Access

☐ HTTPS ☒ PING ☐ HTTP ☒ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ FCT-Access  
☒ Auto IPsec Request

DHCP Server

☐ Enable

Security Mode

None

Device Management

Detect and Identify Devices

☐

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

☐

Comments

Write a comment...

0/255

Administrative Status

☒ Up ☐ Down

4

OK

Cancel

Go to **Router > Static > Static Routes** and create a new route as shown:

Destination IP/Mask

0.0.0.0/0.0.0.0 1

Device

wan1 2

Gateway

10.0.10.254 3

Distance

10 (1-255, Default=10)

Priority

0 (0-4294967295)

Comments

Write a comment...

0/255

4

OK

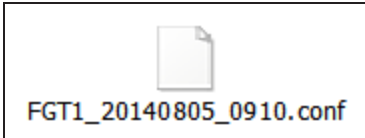
Cancel

## 5. Configuring your firewall policies

Go to **Policy & Objects > Policy > IPv4** and configure firewall policies as desired.

## 6. Replicate the entire configuration on the second device

Once the first FortiGate is configured, the easiest way to configure the second one is to backup the configuration file of the first FortiGate and restore it on the second.



You can change the hostname and HA priority lines directly in the configuration file prior to restoring it on the second FortiGate.

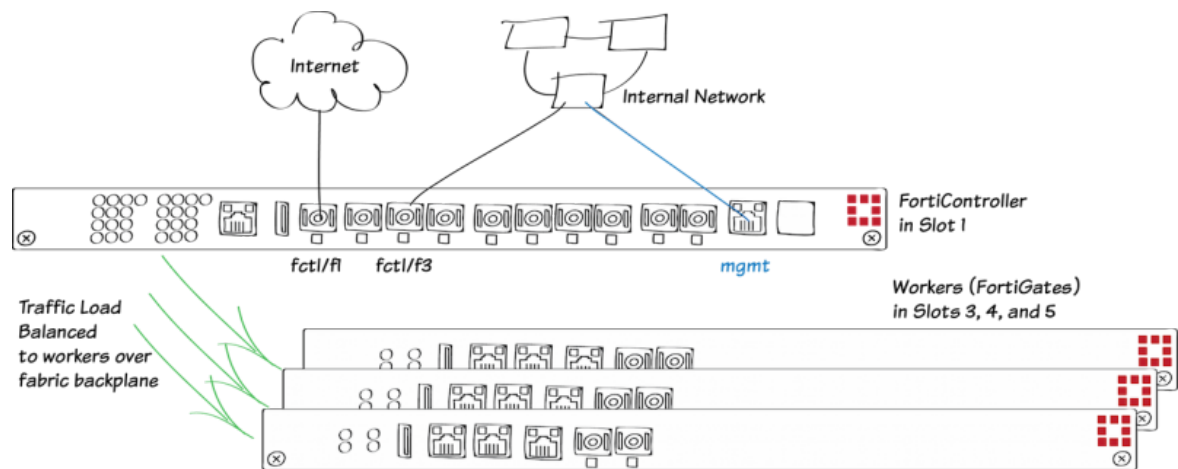
*Do not use a text editor, like Notepad or Word, to do this editing. Instead, use a code editor, like Notepad++ or TextWrangler, that won't add unintended content to the file.*

Go to **System > Dashboard > Status** and select **Backup** next to **System Configuration** in the **System Information** widget.

|                       |   |
|-----------------------|---|
| Firmware Version      | v5.2.0,build0589 (GA) [Update] [Details]      |
| System Configuration  | [Backup] [Restore] [Revisions]                |
| Current Administrator | admin [Change Password] /2 in Total [Details] |

For further reading, check out [High Availability](#) in the [FortiOS 5.2 Handbook](#).

# SLBC setup with one FortiController-5103B



This example describes the basics of setting up a Session-aware Load Balancing Cluster (SLBC) that consists of one FortiController-5103B, installed in chassis slot 1, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight 10 Gbit network connections.

For more information about SLBC go [here](#).

## 1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiController in slot 1. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally. (To check normal operation LED status see the FortiGate-5000 series documents available [here](#).)

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiController

Connect to the FortiController GUI (using HTTPS) or CLI (using SSH) with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None). Login using the admin administrator account and no password.

Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
edit admin
set password <password>
end
```

Change the FortiController mgmt interface IP address. From the GUI use the **Management Port** widget or from the CLI enter this command.

```
config system interface
edit mgmt
set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
edit route 1
set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
set chassis-type fortigate-5140
end
```

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. Since the workers have not been configured yet their status is **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

You can also enter the following CLI command to configure the external management IP/Netmask and management access to this address:

### 3. Adding the workers

Enter this command to reset the workers to factory default settings.

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

Config

Member Management

External Management IP/Netmask192.168.1.101/255.255.255.0

Internal Management Network10.101.10.0/255.255.255.0

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FGFM

☐ SSH

☐ SNMP

☐ TELNET

Apply

Membership

Edit

| Worker Blade | Role   | Weight | Status      |             |
|--------------|--------|--------|-------------|-------------|
| Slot #3      | Active | 5      | <div></div> | <div></div> |
| Slot #4      | Active | 5      | <div></div> | <div></div> |
| Slot #5      | Active | 5      | <div></div> | <div></div> |

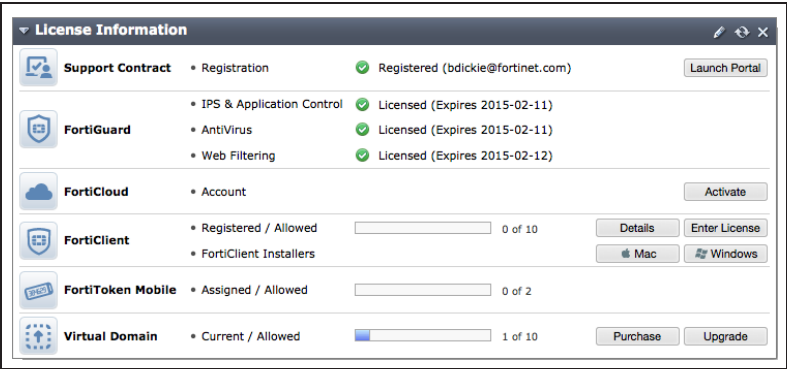
```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

```
config load-balance setting
endset base-mgmt-external-ip 172.20.120.100 255.255.255.0
endset base-mgmt-allowaccess https ssh ping
end
```

```
execute factoryreset
```



Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**. You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers.

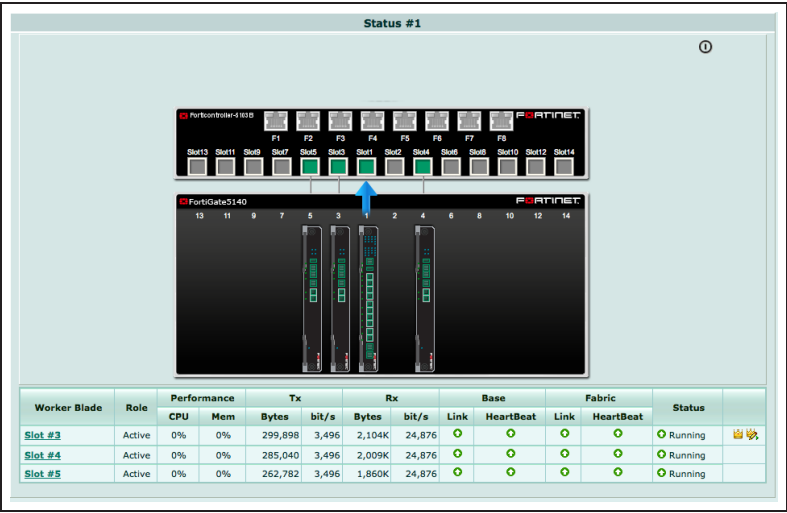


Log into the CLI of each worker and enter this CLI command to set the worker to operate in FortiController mode.

```
config system elbc
set mode forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

The worker in the lowest slot number usually becomes the primary unit.



## 4. Results

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP you connect to the primary worker. When you make configuration changes they are

synchronized to all workers in the cluster.

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the Internet to FortiController front panel interface 4 (fctrl/f4 on the worker GUI and CLI) and an internal network to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) . Then enter the root VDOM and add a policy to allow users on the Internal network to access the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | fctrl/f3        | + |
| Source Address      | Internal-net    | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | fctrl/f1        | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

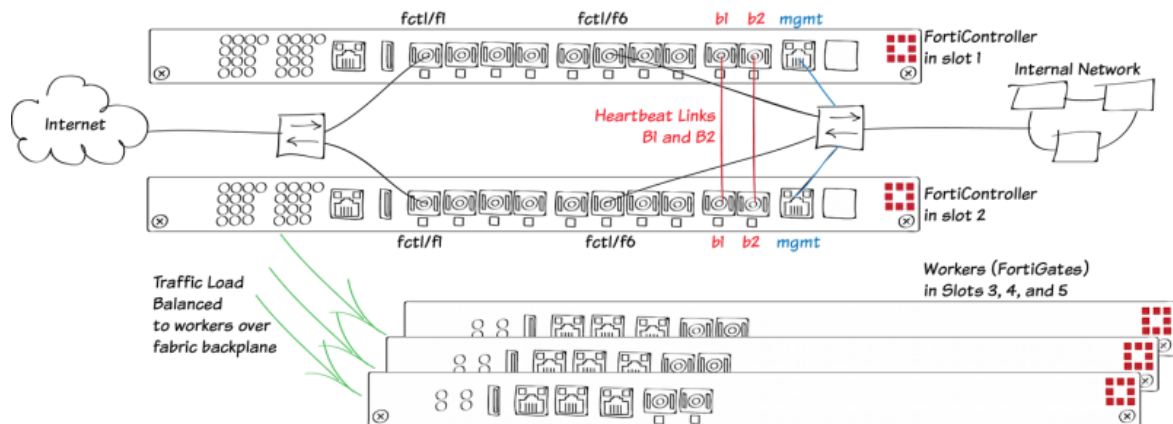
☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

For further reading, check out the [FortiController Session-aware Load Balancing Guide](#).

# SLBC Active-Passive setup with two FortiController-5103Bs



This example describes the basics of setting up an active-passive Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight redundant 10Gbit network connections.

The FortiControllers in the same chassis to operate in active-passive HA mode for redundancy. The FortiController in slot 1 becomes the primary unit actively processing sessions. The FortiController in slot 2 becomes the subordinate unit, sharing the primary unit's session table. If the primary unit fails the subordinate unit resumes all active sessions.

All networks have redundant connections to both FortiControllers. You also create heartbeat links between the FortiControllers and management links from the FortiControllers to an internal network.

For more information about SLBC go [here](#).

## 1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create duplicate connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the GUI **Administrators** widget or enter this CLI command.

```
config admin user
edit admin
set password <password>
end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter this command. Each FortiController should have a different Management IP address.

```
config system interface
edit mgmt
set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
edit 1
set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
set chassis-type fortigate-5140
end
```

Configure active-passive HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

The screenshot shows the 'High Availability' configuration window. At the top is a table titled 'Cluster Members' with columns: Host Name, SN, Role, IP, Up Time, The number of link-up Port, Worker Failure, In Sync, Elbc sync. Below this is the 'Configure' section. It includes a 'Mode' dropdown set to 'Active-Passive', a 'Device Priority (0-255)' field set to '128', a 'Group ID(0-31)' field set to '23', an 'Enable Override' checkbox (unchecked), a 'Heartbeat interval(200-1000ms)' field set to '250', a 'Number of heartbeats lost(2-255)' field set to '5', a 'VLAN to use for HA heartbeat traffic(1-4094)' field set to '999', and an 'Enable Chassis Redundancy' checkbox (unchecked). At the bottom, there are two columns: 'Available' and 'Selected'. The 'Available' column contains 'mgmt'. The 'Selected' column contains 'b1' and 'b2'. Green arrows point from 'mgmt' to 'b1' and 'b2'. At the bottom of the window are 'OK' and 'Cancel' buttons.

You can also enter this command:

```
config system ha
set mode a-p
set groupid 23
set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the

FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form an active-passive cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of all FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

| Host Name        | SN               | Role   | IP             | Up Time | The number of link-up | Port Worker Failure | In Sync | Elbic sync |
|------------------|------------------|--------|----------------|---------|-----------------------|---------------------|---------|------------|
| FTS13B3912000029 | FTS13B3912000029 | Master | 169.254.128.81 | 545.32  | 0                     | 0/0                 | 1       | 1          |
| FTS13B3912000051 | FTS13B3912000051 | Slave  | 169.254.128.82 | 405.77  | 0                     | 0/0                 | 1       | 1          |

Configure

Mode

Active-Passive

Device Priority (0-255)

128

Group ID(0-31)

10

Enable Override

☐

Heartbeat interval(200-1000ms)

250

Number of heartbeats lost(2-255)

5

VLAN to use for HA heartbeat traffic(1-4094)

999

Enable Chassis Redundancy

☐

Available

mgmt

Selected

b1  
b2

Heartbeat Device

OK

Cancel

You can also go to **Load Balance > Status** to see the status of the cluster.

This page should show both FortiControllers in the cluster.

The FortiController in slot 1 is the primary unit (slot icon colored green) and the FortiController in slot 2 is the backup unit (slot icon colored yellow).

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

You can also enter this command to add slots 3, 4, and 5 to the cluster:

You can also enter this command to set the external management IP/Netmask and configure management access.

Enable base management traffic between FortiControllers.

Enable base control traffic between FortiControllers.

If the workers are going to run FortiOS

Config

Member Management

External Management IP/Netmask192.168.1.101/255.255.255.0

Internal Management Network10.101.10.0/255.255.255.0

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FGFM

☐ SSH

☐ SNMP

☐ TELNET

Apply

Membership

Edit

| Worker Blade | Role   | Weight | Status      |             |
|--------------|--------|--------|-------------|-------------|
| Slot #3      | Active | 5      | <div></div> | <div></div> |
| Slot #4      | Active | 5      | <div></div> | <div></div> |
| Slot #5      | Active | 5      | <div></div> | <div></div> |

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
end
```

```
config load-balance setting
config base-mgmt-interfaces
edit b1
next
edit b2
end
end
```

```
config load-balance setting
config base-ctrl-interfaces
edit b1
next
edit b2
```

Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

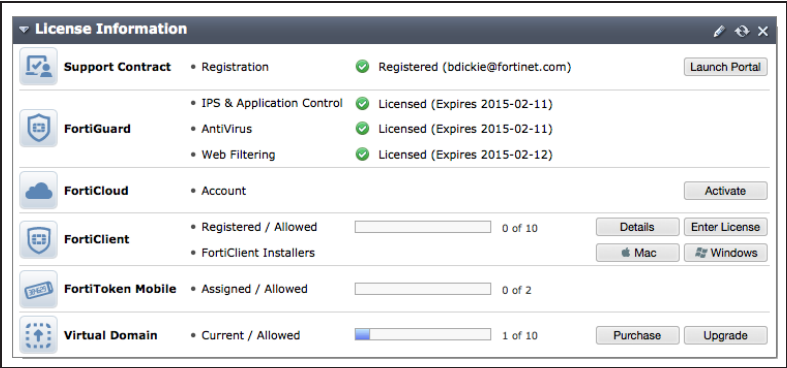
```
end
end
```

### 3. Adding the workers to the cluster

Reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**. You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers.



Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

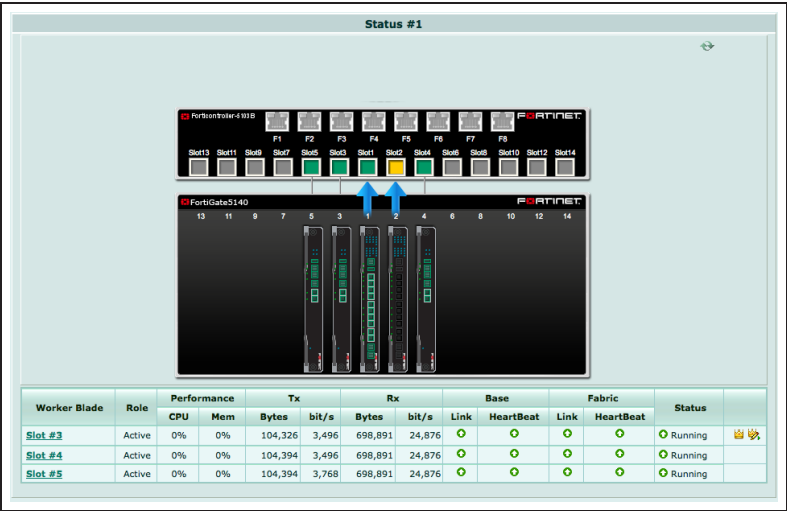
Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
  set mode forticontroller
end
```



The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.



## 4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

Incoming Interface

fctrl/f6

+

Source Address

Internal-net

+

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

fctrl/f1

+

Destination Address

all

+

Schedule

always

+

Service

ALL

+

Action

ACCEPT

+

Firewall / Network Options

ON NAT

Use Outgoing Interface Address

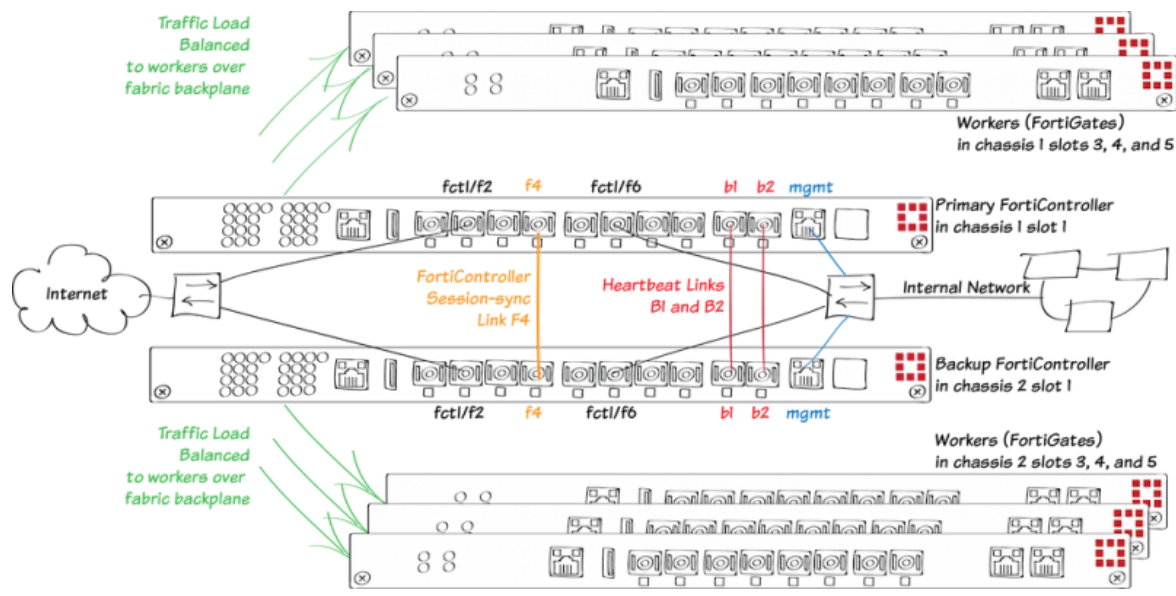
Fixed Port

Use Dynamic IP Pool

Click to add...

For further reading, check out the  
**FortiController Session-aware Load  
Balancing Guide.**

# SLBC Active-Passive with two FortiController-5103Bs and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, two FortiController-5103Bs, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The FortiController in chassis 2 slot 1 becomes the subordinate unit. If the primary unit fails the subordinate unit resumes all active sessions.

All networks in this example have redundant connections to both FortiControllers and redundant heartbeat and base control and management links are created between the FortiControllers using their front panel B1 and B2 interfaces.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface.)

Heartbeat and base control and management traffic uses VLANs and specific subnets. So the switches and network components used must be configured to allow traffic on these VLANs and you should be aware of the subnets used in case they conflict with any connected networks.

This example sets the device priority of the FortiController in chassis 1 higher than the device priority of the FortiController in chassis 2 to make sure that the FortiController in chassis 1 becomes the primary FortiController for the cluster.

For more information about SLBC go [here](#).

## 1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install a FortiController in slot 1 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create duplicate connections from both FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiController in Chassis 1

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the GUI or enter this command.

```
config admin user
  edit admin
    set password
  end
```

Change the FortiController mgmt interface IP address. Use the GUI **Management Port** widget or enter this command.

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

If you need to add a default route for the management IP address, enter this command.

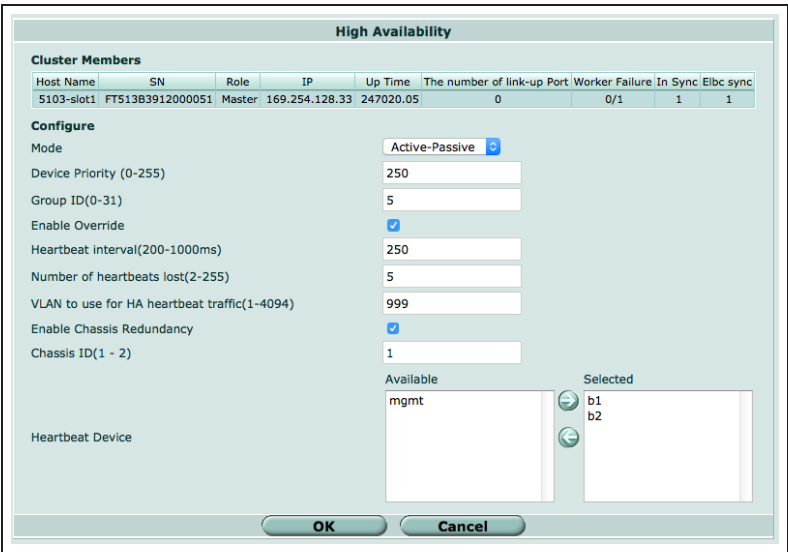
```
config route static
  edit 1
    set gateway 172.20.120.2
  end
```

Set the chassis type that you are using.

```
config system global
  set chassis-type fortigate-5140
end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.



Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
  set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command.

```
config system ha
```

```

        set mode active-passive
set groupid 5
        set priority 250
        set override enable
        set chassis-redundancy enable
        set chassis-id 1
        set hbdev b1 b2
        set session-sync-port f4
end

```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

**Enable Override** is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

### 3. Configuring the FortiController in Chassis 2

Log into the FortiController in chassis 2.

Enter these commands to set the host name to ch2-slot1 and duplicate the HA configuration of the FortiController in chassis 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```

config system global
    set hostname ch2-slot1
end

config system ha
    set mode active-passive
    set groupid 5
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end

```

## 4. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. Both FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to the FortiController in chassis 1.

The FortiController in chassis 2 becomes the backup FortiController. You cannot log into or manage the backup FortiController until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiController. This is described below. (You can also connect to the backup FortiController CLI using the console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.

*Note in some of the screen images in this example the host names shown on the screen images may not match the host names used in the example configuration.*

High Availability

Cluster Members

| Host Name        | SN               | Role   | IP             | Up Time | The number of link-up Port | Worker Failure | In Sync | Elbc sync |
|------------------|------------------|--------|----------------|---------|----------------------------|----------------|---------|-----------|
| FTS13B3912000029 | FTS13B3912000029 | Master | 169.254.128.81 | 357.50  | 0                          | 0/0            | 1       | 1         |
| FTS13B3912000051 | FTS13B3912000051 | Slave  | 169.254.128.82 | 53.84   | 0                          | 0/0            | 0       | 1         |

Configure

Mode

Active-Passive

Device Priority (0-255)

128

Group ID(0-31)

10

Enable Override

☐

Heartbeat interval(200-1000ms)

250

Number of heartbeats lost(2-255)

5

VLAN to use for HA heartbeat traffic(1-4094)

999

Enable Chassis Redundancy

☒

Chassis ID(1 - 2)

1

Available

mgmt

Selected

b1  
b2

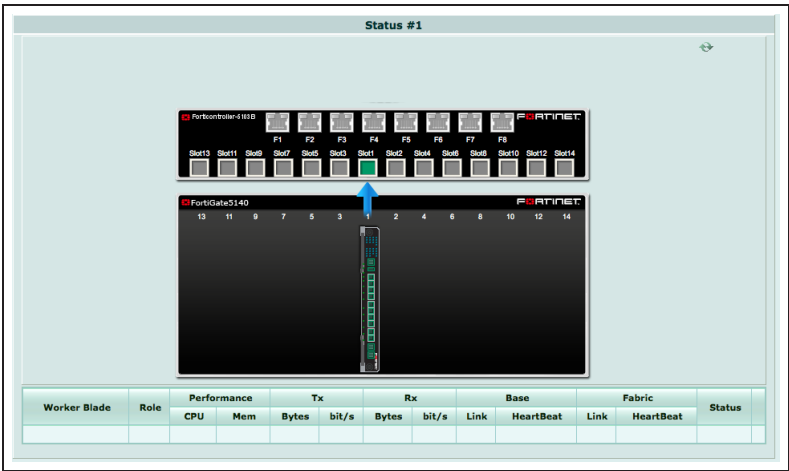
Heartbeat Device

OK

Cancel



You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).

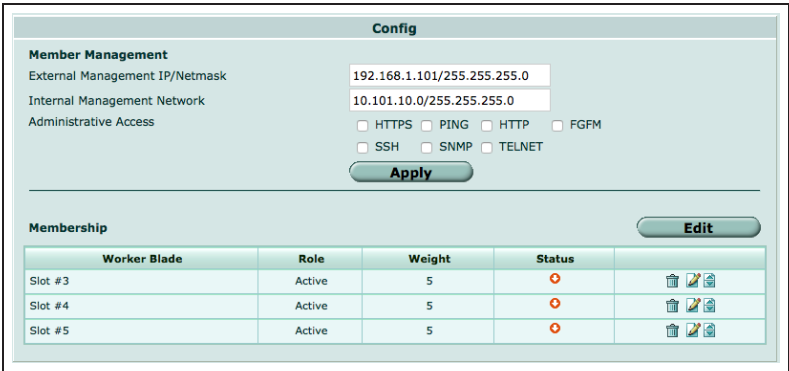


Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

You can also enter this command to add slots 3, 4, and 5 to the cluster.



```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

You can also enter this command to set the External Management IP and configure management access.

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
config base-mgmt-interfaces
edit b1
next
edit b2
end
end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
config base-ctrl-interfaces
edit b1
next
edit b2
end
end
```

## 5. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

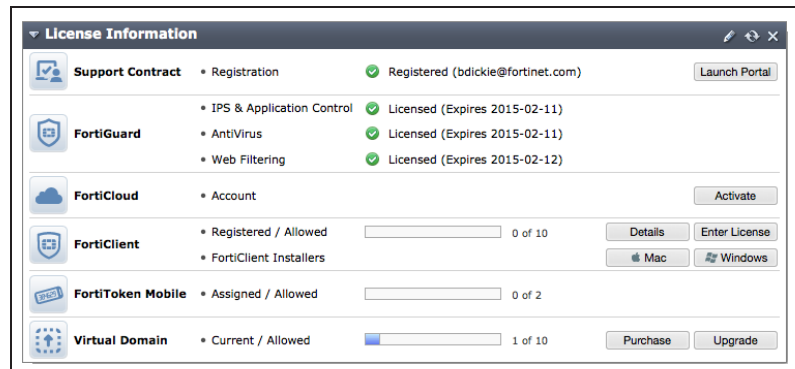
```
config system interface
edit mgmt1
set ip 172.20.120.120
end
```

Optionally give each worker a different hostname. The hostname is

```
config system global
set hostname worker-chassis-1-slot-3
```

also not synchronized and allows you to identify each worker. end

Register and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**. You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed third-party certificates are synchronized to all of the workers.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
set mode forticontroller
end
```

## 6. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiController. Some examples:

- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 1, browse to: **https://172.20.120.100:44311**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, (the backup FortiController) browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 1 slot 4: **telnet 172.20.120.100 2314**
- To use SSH to connect to the CLI the worker in chassis 2 slot 5: **ssh admin@172.20.120.100 -p2225**
- To use SNMP to query the FortiController in chassis 2 slot 1 (the backup FortiController) use port **16121** in the SNMP query.

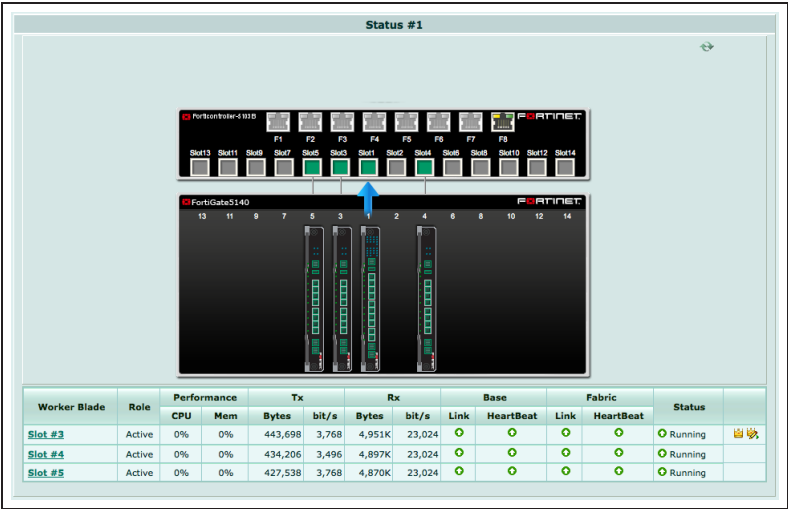
You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you

first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiController is by using its special port number.

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

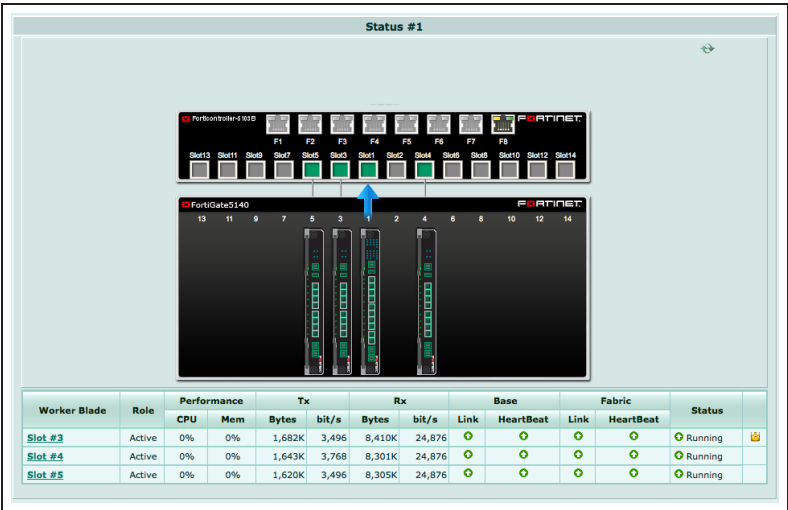
On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Log into the backup FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**. As the workers in chassis 2 restart they should appear in their appropriate slots.

The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



## 7. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel 2 interfaces (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel 6 interfaces (fctrl/f6) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | fctrl/f6        | + |
| Source Address      | Internal_NET    | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | fctrl/f2        | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 8. Results - Checking the cluster status

You can use the following get and diagnose commands to show the status of the cluster and all of the devices in it.

Log into the **primary FortiController** CLI and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211
```

```
get system status
Version: FortiController-5103B
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sat Sep 13 06:51:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]

Slot 3: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
Slot 4: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
Slot 5: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
```

Enter this command from the primary FortiController to show the HA status of the primary and backup FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.41,
uptime=62581.81, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=          b1 best=yes
                        local_interface=          b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=1), ip=169.254.128.42,
uptime=1644.71, chassis=2(1)
    slot: 1
    sync: conf_sync=0, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=          b1 last_hb_time=66430.35
status=alive
    local_interface= b2 last_hb_time= 0.00    status=dead
```

**Log into the backup FortiController CLI and enter this command to view the status of the backup FortiController.**

**To use SSH:**

```
ssh admin@172.20.120.100 -p2221
```

```
get system status
  Version: FortiController-5103B
v5.0,build0020,131118 (Patch 3)
  Branch Point: 0020
  Serial-Number: FT513B3912000051
  BIOS version: 04000009
  System Part-Number: P08442-04
  Hostname: ch2-slot1
  Current HA mode: a-p, backup
  System time: Sat Sep 13 07:29:04 2014
```

```
Daylight Time Saving: Yes
Time Zone: (GMT-8:00) Pacific Time (US&Canada)
```

Enter this command to view the status of the backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]

Slot  3: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot  4: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot  5: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
```

Enter this command from the backup FortiController to show the HA status of the backup and primary FortiControllers. Notice that the backup FortiController is shown first. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

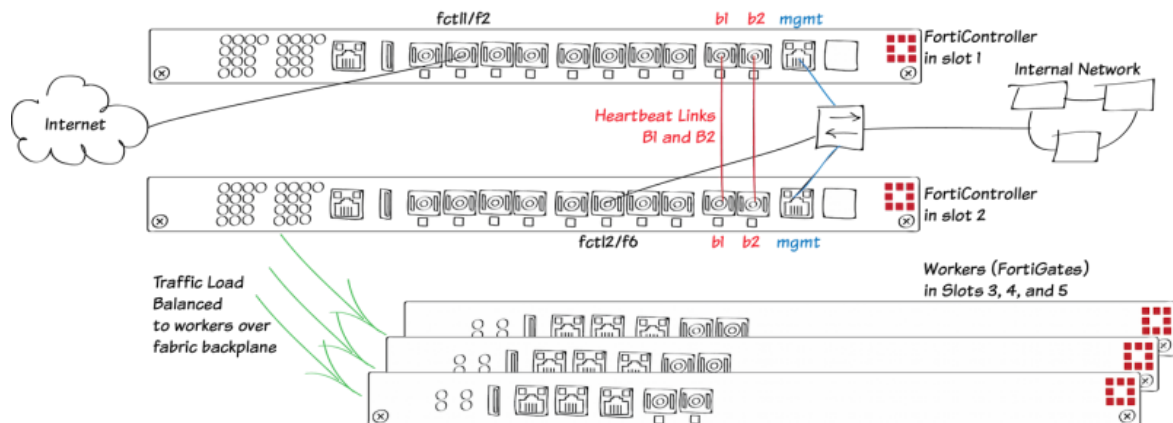
```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1 (FT513B3912000051), Slave (priority=1), ip=169.254.128.42,
uptime=3795.92, chassis=2 (1)
  slot: 1
  sync: conf_sync=0, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 best=yes
  local_interface=      b2 best=no
```



```
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.41,  
uptime=64732.98, chassis=1(1)  
  slot: 1  
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)  
  session: total=0, session_sync=in sync  
  state: worker_failure=0/3, intf_state=(port up:)=0  
force-state(0:none) hbdevs: local_interface=      b1 last_hb_time=68534.90  
status=alive  
  local_interface=      b2 last_hb_time=      0.00  status=dead
```

For further reading, check out the  
**FortiController Session-aware Load  
Balancing Guide.**

# SLBC Dual Mode with two FortiController-5103Bs



This example describes the basics of setting up a dual mode Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to 16 10Gbit network connections.

The two FortiControllers in the same chassis to operate in dual mode to double the number of network interfaces available. In dual mode, two FortiControllers load balance traffic to multiple workers. Traffic can be received by both FortiControllers and load balanced to all of the workers in the chassis. In dual mode configuration the front panel interfaces of both FortiControllers are active.

In a dual FortiController-5103B cluster this means up to 16 10Gbyte network interfaces are available. The interfaces of the FortiController in slot 1 are named fctrl/f1 to fctrl/f8 and the interfaces of the FortiController in slot 2 are named fctrl2/f1 to fctrl2/f8.

All networks have single connections to the first or second FortiController. One or more heartbeat links are created between the FortiControllers. Redundant heartbeat links are recommended. The heartbeat links use the front panel B1 and B2 interfaces.

If one of the FortiControllers fails, the remaining FortiController keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

For more information about SLBC go [here](#).

## 1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the **Administrators** widget in the GUI or enter the following command in the CLI.

```
config admin user
edit admin
set password password
end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter the following command in the CLI.

```
config system interface
edit mgmt
set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this

```
config route static
edit 1
set gateway 172.20.120.2
```

command.

Set the chassis type that you are using.

Configure dual Mode HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Dual Mode**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

```
end

config system global
    set chassis-type fortigate-5140
end
```

You can also enter this CLI command:

```
config system ha
    set mode dual
    set groupid 4
    set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it

conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form a dual mode cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of the FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

| Host Name        | SN               | Role   | IP             | Up Time | The number of link-up Port | Worker Failure | In Sync | Elb sync |
|------------------|------------------|--------|----------------|---------|----------------------------|----------------|---------|----------|
| FT513B3912000029 | FT513B3912000029 | Master | 169.254.128.33 | 1894.42 | 0                          | 0/0            | 1       | 1        |
| FT513B3912000051 | FT513B3912000051 | Slave  | 169.254.128.34 | 827.73  | 0                          | 0/0            | 1       | 1        |

Configure

Mode

Dual Mode

Device Priority (0-255)

128

Group ID(0-31)

4

Enable Override

☐

Heartbeat interval(200-1000ms)

250

Number of heartbeats lost(2-255)

5

VLAN to use for HA heartbeat traffic(1-4094)

999

Enable Chassis Redundancy

☐

Heartbeat Device

Available

mgmt

Selected

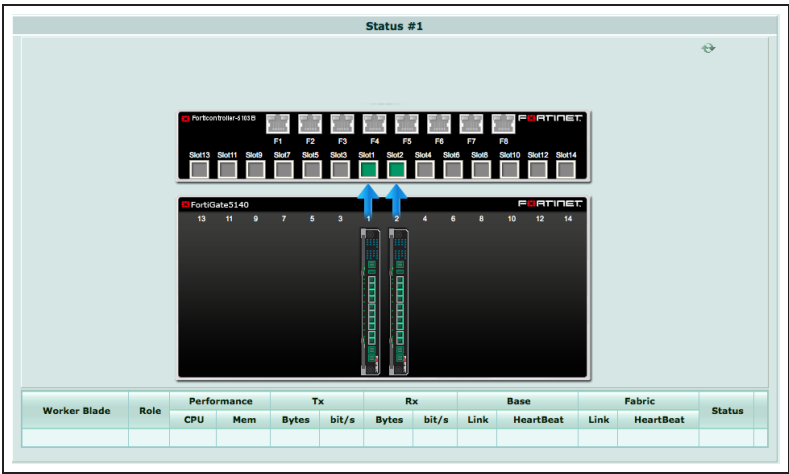
b1  
b2

OK

Cancel

You can also go to **Load Balance > Status** to see the status of the cluster. This page should show both FortiControllers in the cluster.

Since both FortiControllers are active their slot icons are both colored green.

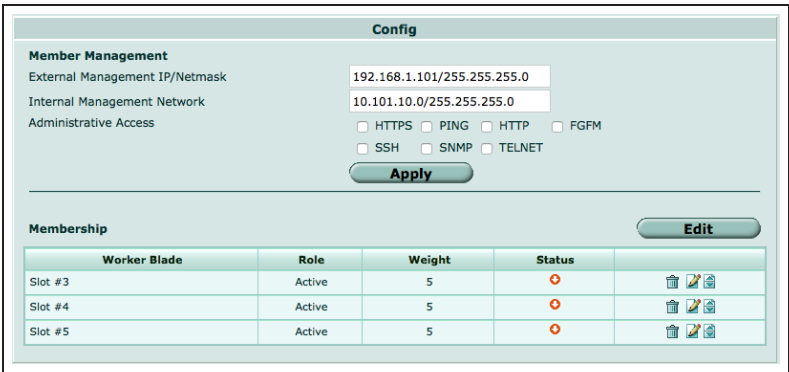


Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

You can also enter this command to add slots 3, 4, and 5 to the cluster.



```
config load-balance setting
config slots
    edit 3
    next
    edit 4
    next
    edit 5
    end
end
```

You can also enter this command to configure the external management IP/Netmask and management access to

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
```

this address. `end`

Enable base management traffic between FortiControllers.

```
config load-balance setting
config base-mgmt-interfaces
    edit b1
    next
    edit b2
    end
end
```

Enable base control traffic between FortiControllers.

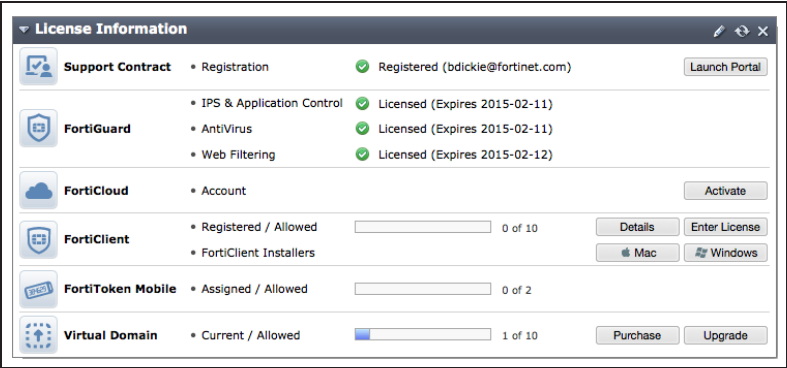
```
config load-balance setting
config base-ctrl-interfaces
    edit b1
    next
    edit b2
    end
end
```

### 3. Adding the workers to the cluster

Reset the workers to factory default settings. `execute factoryreset`

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**. You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers.



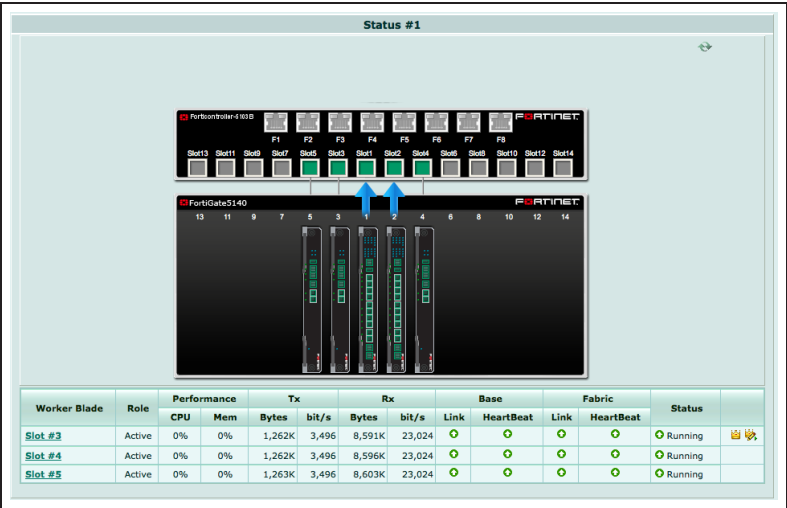
Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
  set mode dual-forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.





## 4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 of the FortiController in slot 1 (fctr1/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 of the FortiController in slot 2 (fctr2/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | fctr2/f6        | + |
| Source Address      | Internal_NET    | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | fctr1/f2        | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

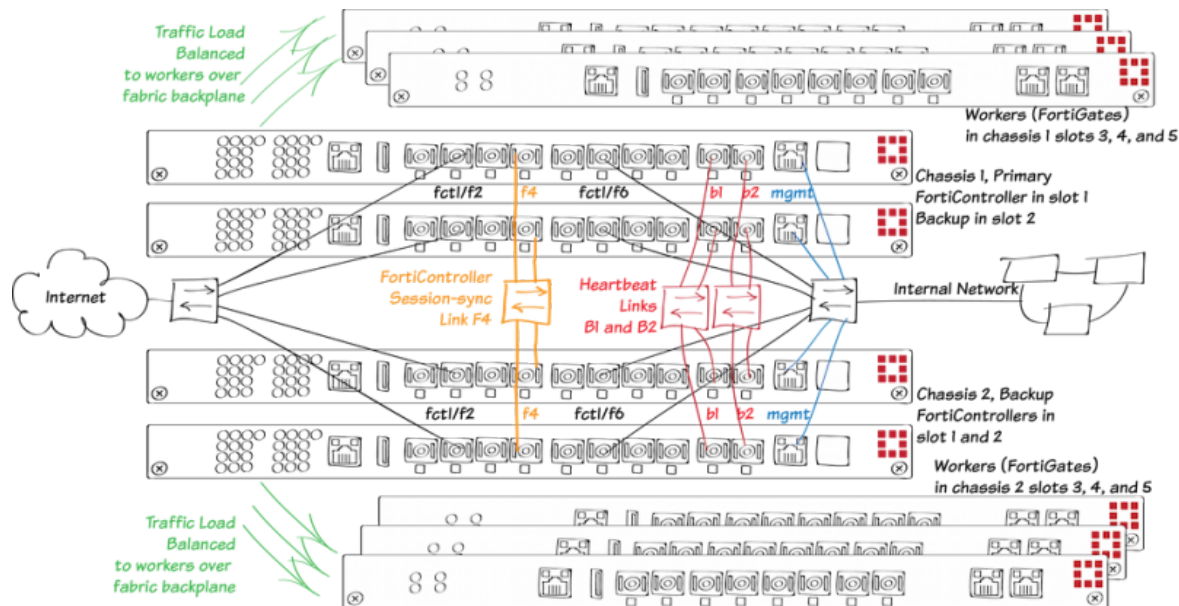
☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

For further reading, check out the  
**FortiController Session-aware Load  
Balancing Guide.**

# SLBC Active-Passive with four FortiController-5103Bs and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, four FortiController-5103Bs two in each chassis, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The other FortiControllers become the subordinate units.

In active-passive HA with two chassis and four FortiControllers, both chassis have two FortiControllers in active-passive HA mode and the same number of workers. Network connections are duplicated to the redundant FortiControllers in each chassis and between chassis for a total of four redundant data connections to each network.

All traffic is processed by the primary unit. If the primary unit fails, all traffic fails over to the chassis with two functioning FortiControllers and one of these FortiControllers becomes the new primary unit and processes all traffic. If the primary unit in the second chassis fails as well, one of the remaining FortiControllers becomes the primary unit and processes all traffic.

Heartbeat and base control and management communication is established between the chassis using the FortiController B1 and B2 interfaces. Only one heartbeat connection is required but redundant connections are recommended. Connect all of the B1 and all of the B2 interfaces together using switches. This example shows using one switch for the B1 connections and another for the B2 connections. You could also use one switch for both the B1 and B2 connections but using separate switches provides more redundancy.

The following VLAN tags and subnets are used by traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface, F4 is used in this example to make the diagram clearer.) FortiController-5103B session sync traffic uses VLAN 2000.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

For more information about SLBC go [here](#).

# 1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install FortiControllers in slot 1 and 2 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create redundant connections from all four FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces together.

Connect the mgmt interfaces of all of the FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiControllers and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiController in Chassis 1 Slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the GUI or enter this command.

```
config admin user
    edit admin
        set password
    end
```

Change the FortiController mgmt interface IP address. Use the GUI **Management Port** widget or enter this command.

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit 1
    set gateway 172.20.120.2
  end
```

Set the chassis type that you are using.

```
config system global
  set chassis-type fortigate-5140
end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

**High Availability**

**Cluster Members**

| Host Name  | SN               | Role   | IP             | Up Time   | The number of link-up Port | Worker Failure | In Sync | Elbc sync |
|------------|------------------|--------|----------------|-----------|----------------------------|----------------|---------|-----------|
| 5103-slot1 | FT513B3912000051 | Master | 169.254.128.33 | 247020.05 | 0                          | 0/1            | 1       | 1         |

**Configure**

Mode: Active-Passive

Device Priority (0-255): 250

Group ID(0-31): 5

Enable Override: ☒

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Available: mgmt

Selected: b1, b2

Heartbeat Device

OK Cancel

Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
  set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command.

```
config system ha
set mode active-passive
set groupid 15
set priority 250
set override enable
set chassis-redundancy enable
set chassis-id 1
set hbdev b1 b2
set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

### 3. Configuring the FortiController in Chassis 1 Slot 2

Log into the FortiController in chassis 1 slot 2.

```
config system global
set hostname ch1-slot2
end
```

Enter these commands to set the host name to ch1-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10).

```
config system interface
edit mgmt
set ip 172.20.120.152/24
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system ha
set mode active-passive
set groupid 15
set priority 10
set chassis-redundancy enable
set chassis-id 1
set hbdev b1 b2
set session-sync-port f4
end
```

## 4. Configuring the FortiController in Chassis 2 Slot 1

Log into the FortiController in chassis 2 slot 1.

Enter these commands to set the host name to ch2-slot1, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
    set hostname ch2-slot1
end

config system interface
    edit mgmt
        set ip 172.20.120.251/24
    end

config system ha
    set mode active-passive
    set groupid 15
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

## 5. Configuring the FortiController in Chassis 2 Slot 2

Log into the FortiController in chassis 2 slot 2.

Enter these commands to set the host name to ch2-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
    set hostname ch2-slot2
end

config system interface
    edit mgmt
        set ip 172.20.120.252/24
    end

config system ha
    set mode active-passive
    set groupid 15
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

## 6. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become backup FortiControllers. You cannot log into or manage the backup FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiControllers. This is described below. (You can also connect to any backup FortiController CLI using their console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.

High Availability

Cluster Members

| Host Name | SN               | Role   | IP              | Up Time | The number of link-up Port | Worker Failure | In Sync | Elbc sync |
|-----------|------------------|--------|-----------------|---------|----------------------------|----------------|---------|-----------|
| ch1-slot1 | FT513B3912000029 | Master | 169.254.128.121 | 1075.00 | 0                          | 0/3            | 1       | 1         |
| ch2-slot1 | FT513B3912000051 | Slave  | 169.254.128.124 | 423.61  | 0                          | 0/0            | 0       | 0         |
| ch2-slot2 | FT513B3913000168 | Slave  | 169.254.128.123 | 273.87  | 0                          | 0/3            | 0       | 1         |
| ch1-slot2 | FT513B3914000006 | Slave  | 169.254.128.122 | 703.38  | 0                          | 0/3            | 1       | 1         |

Configure

Mode

Active-Passive

Device Priority (0-255)

250

Group ID(0-31)

5

Enable Override

☒

Heartbeat interval(200-1000ms)

250

Number of heartbeats lost(2-255)

5

VLAN to use for HA heartbeat traffic(1-4094)

999

Enable Chassis Redundancy

☒

Chassis ID(1 - 2)

1

Available

mgmt

Selected

b1  
b2

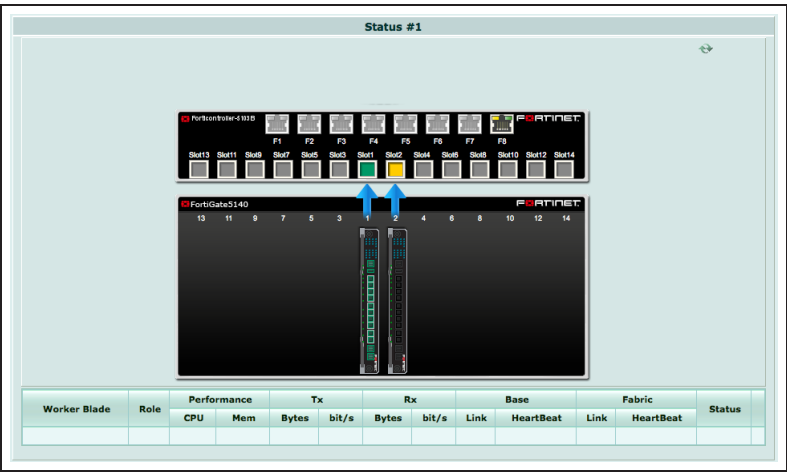
Heartbeat Device

OK

Cancel



You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).

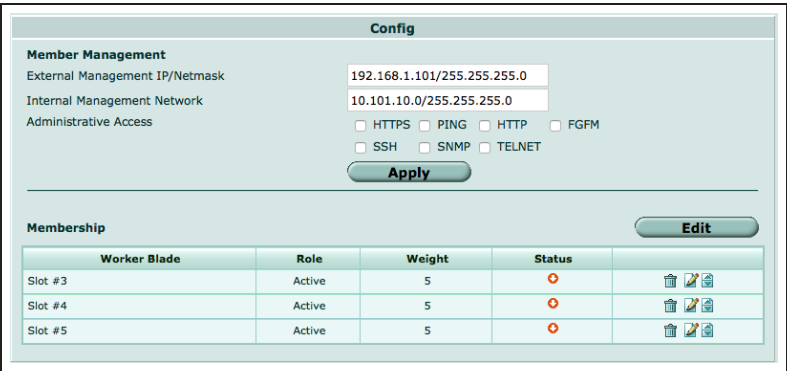


Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

You can also enter this command to add slots 3, 4, and 5 to the cluster.



```
config load-balance setting
config slots
  edit 3
  next
  edit 4
  next
  edit 5
  end
end
```

You can also enter this command to set the External Management IP and configure management access.

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
config base-mgmt-interfaces
edit b1
next
edit b2
end
end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
config base-ctrl-interfaces
edit b1
next
edit b2
end
end
```

## 7. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

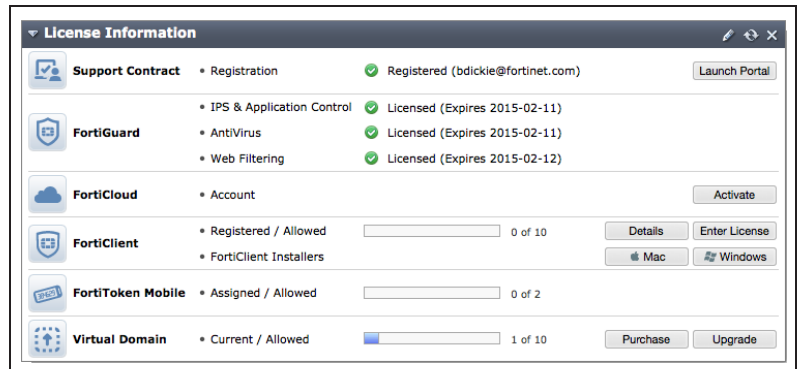
Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
edit mgmt1
set ip 172.20.120.120
end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
set hostname worker-chassis-1-slot-3
end
```

Register each worker and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**. You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
set mode forticontroller
end
```

## 8. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiControllers. Some examples:

- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 2, browse to: **https://172.20.120.100:44312**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 2 slot 4: **telnet 172.20.120.100 2324**
- To use SSH to connect to the CLI the worker in chassis 1 slot 5: **ssh admin@172.20.120.100 -p2215**
- To use SNMP to query the FortiController in chassis 1 slot 2 use port **16112** in the SNMP query.

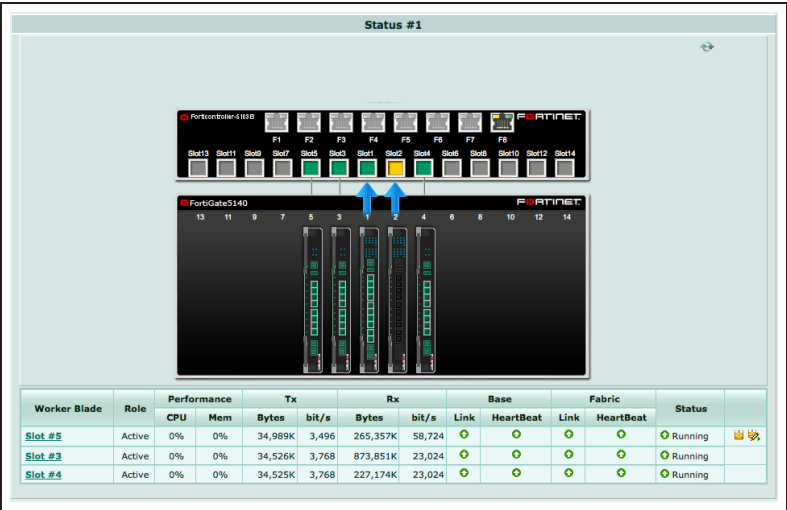
You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiControllers is by using its special port number (or a serial connection to the Console port).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP

manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

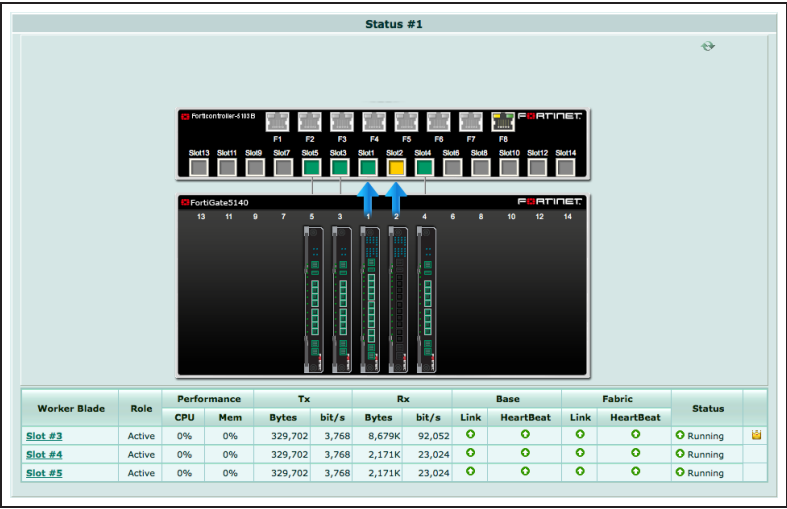
On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Log into a backup FortiController GUI (for example by browsing to <https://172.20.120.100:44321> to log into the FortiController in chassis 2 slot 1) and go to **Load Balance > Status**. If the workers in chassis 2 are configured correctly they should appear in their appropriate slots.

The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



## 9. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6) you can access the root VDOM and add a policy to allow users on the Internal network to access the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | fctrl/f6        | + |
| Source Address      | Internal_NET    | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | fctrl/f2        | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 10. Results - Primary FortiController cluster status

Log into the **primary FortiController CLI** and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211
```

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sun Sep 14 08:16:25 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working: 3 [ 3 Active 0 Standby]
  Ready:   0 [ 0 Active 0 Standby]
  Dead:    0 [ 0 Active 0 Standby]
  Total:   3 [ 3 Active 0 Standby]

Slot 3: Status:Working  Function:Active
```

```

Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 4: Status:Working  Function:Active
Link: Base: Up          Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 5: Status:Working  Function:Active
Link: Base: Up          Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"

```

Enter this command from the primary FortiController to show the HA status of the FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4416.18, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1181.62, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4739.97  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=335.79, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0

```

```

force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4739.93    status=alive
                        local_interface=             b2 last_hb_time=   0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4044.46, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4740.03    status=alive
                        local_interface=             b2 last_hb_time=   0.00    status=dead

```

## 11. Results - Chassis 1 Slot 2 FortiController status

Log into the **chassis 1 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2212
```

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:44:58 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

Enter this command to view the status of this backup FortiController and its workers.

```

get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: slot-3
  Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]

    Slot  3: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"

```

```

Slot 4: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 5: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

```

Enter this command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4292.69, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4664.49, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 4958.88  status=alive
                        local_interface=      b2 last_hb_time= 0.00  status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1429.99, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 4958.88  status=alive
                        local_interface=      b2 last_hb_time= 0.00  status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=584.20, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0

```



```
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4958.88    status=alive
                        local_interface=              b2 last_hb_time=    0.00    status=dead
```

## 12. Results - Chassis 2 Slot 1 FortiController status

Log into the **chassis 2 slot 1 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2221
```

```
get system status
```

```
Version: FortiController-5103B v5.0,build0024,140815
```

```
Branch Point: 0024
```

```
Serial-Number: FT513B3912000051
```

```
BIOS version: 04000009
```

```
System Part-Number: P08442-04
```

```
Hostname: ch2-slot1
```

```
Current HA mode: a-p, backup
```

```
System time: Sun Sep 14 12:53:09 2014
```

```
Daylight Time Saving: Yes
```

```
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
```

```
ELBC Master Blade: slot-3
```

```
Confsync Master Blade: N/A
```

```
Blades:
```

```
Working:  3 [  3 Active  0 Standby]
```

```
Ready:    0 [  0 Active  0 Standby]
```

```
Dead:     0 [  0 Active  0 Standby]
```

```
Total:    3 [  3 Active  0 Standby]
```

```
Slot  3: Status:Working  Function:Active
```

```
Link:      Base: Up      Fabric: Up
```

```
Heartbeat: Management: Good  Data: Good
```

```
Status Message:"Running"
```

```
Slot  4: Status:Working  Function:Active
```

```
Link:      Base: Up      Fabric: Up
```

```
Heartbeat: Management: Good  Data: Good
```

```
Status Message:"Running"
```

```
Slot  5: Status:Working  Function:Active
```

```
Link:      Base: Up      Fabric: Up
```

```
Heartbeat: Management: Good  Data: Good
```

```
Status Message:"Running"
```

Enter this command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers.

Notice that the FortiController in chassis 2 slot 1 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1858.71, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5093.30, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 2074.15    status=alive
                           local_interface=      b2 last_hb_time=    0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1013.01, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 2074.15    status=alive
                           local_interface=      b2 last_hb_time=    0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4721.60, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 2074.17    status=alive
                           local_interface=      b2 last_hb_time=    0.00    status=dead
```

## 13. Results - Chassis 2 Slot 2 FortiController status

Log into the **chassis 2 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:  
ssh admin@172.20.120.100 -p2222  
  
get system status

```
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:56:45 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

Enter this command to view the status of the backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]

Slot  3: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  4: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  5: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
```

Enter this command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1276.77, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
```

```

force-state(0:none)    hbdevs: local_interface=    b1 best=yes
                        local_interface=           b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5356.98, chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time= 1363.89  status=alive
                        local_interface=           b2 last_hb_time= 0.00  status=dead

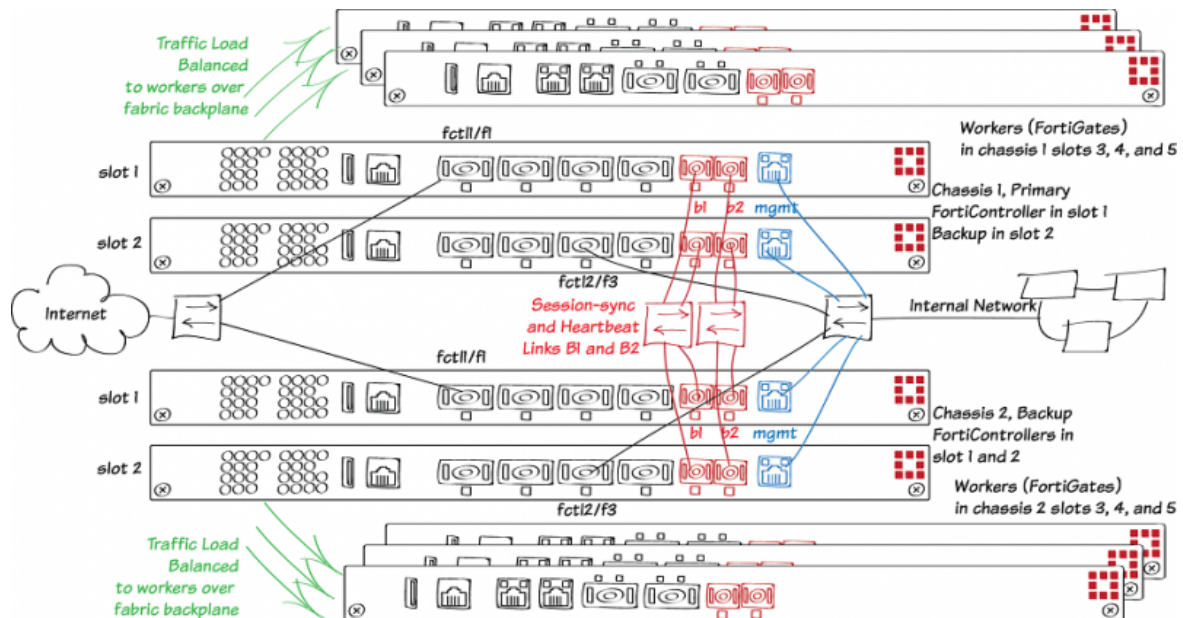
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=2122.58, chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time= 1363.97  status=alive
                        local_interface=           b2 last_hb_time= 0.00  status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4985.27, chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time= 1363.89  status=alive
                        local_interface=           b2 last_hb_time= 0.00  status=dead

```

For further reading, check out the  
**FortiController Session-aware Load  
Balancing Guide.**

# SLBC Dual Mode with two FortiController-5903Cs



This example describes how to setup a dual-mode session-aware load balancing cluster (SLBC) consisting of two FortiGate-5144C chassis, four FortiController-5903Cs two in each chassis, and six FortiGate-5001Ds acting as workers, three in each chassis. This SLBC configuration can have up to 8 redundant 40Gbps network connections. The FortiGate-5144C is required to supply enough power for the FortiController-5903Cs and provide 40Gbps fabric backplane communication.

In this dual mode configuration, the FortiController in chassis 1 slot 1 is configured to become the primary unit. Both of the FortiControllers in chassis 1 receive traffic and load balance it to the workers in chassis 1. In dual mode configuration the front panel interfaces of both FortiControllers are active. All networks have single connections to the FortiController in slot 1 or the FortiController in slot 2. The front panel F1 to F4 interfaces of the FortiController in slot 1 are named fctrl1/f1 to fctrl1/f4 and the front panel F1 to F4 interfaces of the FortiController in slot 2 are named fctrl2/f1 to fctrl2/f4.

The network connections to the FortiControllers in chassis 1 are duplicated with the FortiControllers in chassis 2. If one of the FortiControllers in chassis 1 fails, the FortiController in chassis 2 slot 1 becomes the primary FortiController and all traffic fails over to the FortiControllers in chassis 2. If one of the FortiControllers in chassis 2 fails, the remaining FortiController in chassis 2 keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

Heartbeat, base control, base management, and session sync communication is established between the chassis using the FortiController B1 and B2 interfaces. Connect all of the B1 interfaces together using a 10 Gbps switch.

Collect all of the B2 interfaces together using another 10 Gbps switch. Using the same switch for the B1 and B1 interfaces is not recommended and requires a double VLAN tagging configuration.

The switches must be configured to support the following VLAN tags and subnets used by the traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101
- Session sync traffic uses VLAN 1900 and 1901.

This example sets the device priority of the FortiController in chassis 1 slot 1 is higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

For more information about SLBC go [here](#).

## 1. Hardware setup

Install two FortiGate-5144C series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install FortiControllers in slot 1 and 2 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create redundant network connections to FortiController front panel interfaces. In this example, a redundant connection to the Internet is made to the F1 interface of the FortiController in chassis 1 slot 1 and the F1 interface of the FortiController in chassis 2 slot 1. This becomes the fctl1/f1 interface. As well, a redundant connection to the internal network is made to the F3 interface of the FortiController in chassis 1 slot 2 and the F3 interface of the FortiController in chassis 2 slot 2. This becomes the fctl2/f3 interface.

Create the heartbeat links by connecting the FortiController B1 interfaces together and the FortiController B2 interfaces together.

Connect the mgmt interfaces of all of the FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiControllers and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

## 2. Configuring the FortiController in Chassis 1 Slot 1

This will become the primary FortiController. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 with the default IP address (<https://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the GUI or enter this command.

```
config admin user
    edit admin
        set password <password>
    end
```

Change the FortiController mgmt interface IP address. Use the GUI **Management Port** widget or enter this command.

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit 1
    set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
  set chassis-type fortigate-5144
end
```

Enable FortiController session sync.

```
config load-balance setting
  set session-sync enable
end
```

Configure Dual mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Dual Mode**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

**High Availability**

**Cluster Members**

| Host Name | SN               | Role   | IP             | Up Time | The number of link-up Port | Worker Failure | In Sync | Elbc sync |
|-----------|------------------|--------|----------------|---------|----------------------------|----------------|---------|-----------|
| ch1-slot1 | FT513B3912000051 | Master | 169.254.128.89 | 4772.75 | 0                          | 1/1            | 0       | 1         |

**Configure**

Mode: Dual Mode

Device Priority (0-255): 250

Group ID(0-31): 25

Enable Override: ☒

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Heartbeat Device

Available: mgmt

Selected: b1, b2

OK Cancel

Enter these commands to use the FortiController front panel F4 interface for session sync communication.

```
config system ha
  set session-sync-port f4
end
```



You can also enter the complete HA configuration with this command.

```
config system ha
  set mode dual
  set groupid 25
  set priority 250
  set override enable
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

### 3. Configuring the FortiController in Chassis 1 Slot 2

Log into the FortiController in chassis 1 slot 2.

```
config system global
  set hostname ch1-slot2
end
```

Enter these commands to set the host name to ch1-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10).

```
config system interface
  edit mgmt
    set ip 172.20.120.152/24
  end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system ha
  set mode dual
  set groupid 25
  set priority 10
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
end
```

## 4. Configuring the FortiController in Chassis 2 Slot 1

Log into the FortiController in chassis 2 slot 1.

Enter these commands to set the host name to ch2-slot1, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
    set hostname ch2-slot1
end

config system interface
    edit mgmt
        set ip 172.20.120.251/24
    end

config system ha
    set mode dual
    set groupid 25
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
end
```

## 5. Configuring the FortiController in Chassis 2 Slot 2

Log into the FortiController in chassis 2 slot 2.

Enter these commands to set the host name to ch2-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
    set hostname ch2-slot2
end

config system interface
    edit mgmt
        set ip 172.20.120.252/24
    end

config system ha
    set mode dual
    set groupid 25
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
end
```

## 6. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary FortiController and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become backup FortiControllers. You cannot log into or manage the backup FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiControllers. This is described below. (You can also connect to any backup FortiController CLI using their console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show all four of the FortiControllers in the cluster.

High Availability

Cluster Members

| Host Name | SN               | Role   | IP              | Up Time | The number of link-up Port | Worker Failure | In Sync | Elbc sync |
|-----------|------------------|--------|-----------------|---------|----------------------------|----------------|---------|-----------|
| ch1-slot1 | FT513B3912000029 | Master | 169.254.128.201 | 1095.42 | 0                          | 0/3            | 1       | 1         |
| ch2-slot1 | FT513B3912000051 | Slave  | 169.254.128.203 | 843.96  | 0                          | 0/3            | 1       | 1         |
| ch2-slot2 | FT513B3913000168 | Slave  | 169.254.128.204 | 829.83  | 0                          | 0/3            | 1       | 1         |
| ch1-slot2 | FT513B3914000006 | Slave  | 169.254.128.202 | 861.79  | 0                          | 0/3            | 1       | 1         |

Configure

Mode

Dual Mode

Device Priority (0-255)

128

Group ID(0-31)

25

Enable Override

☐

Heartbeat interval(200-1000ms)

250

Number of heartbeats lost(2-255)

5

VLAN to use for HA heartbeat traffic(1-4094)

999

Enable Chassis Redundancy

☒

Chassis ID(1 - 2)

1

Heartbeat Device

Available

mgmt

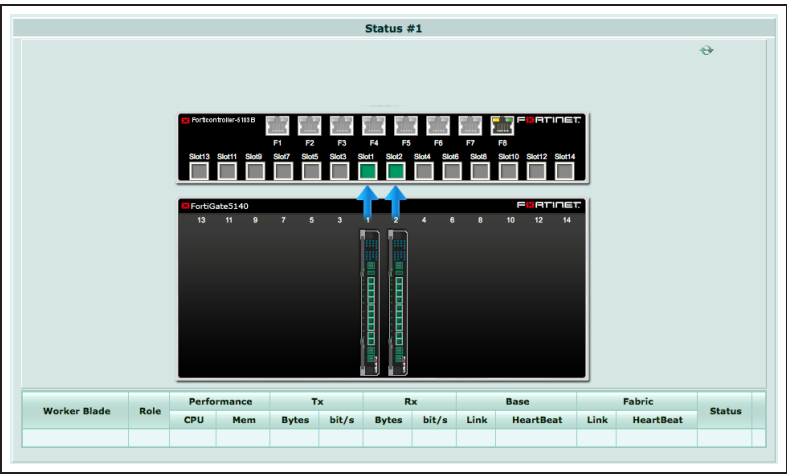
Selected

b1  
b2

OK

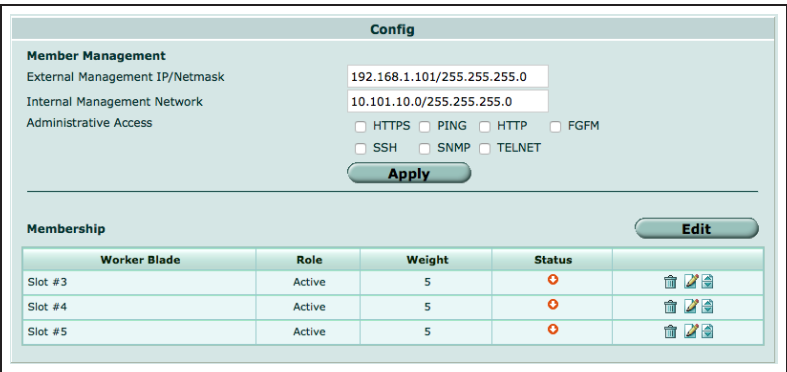
Cancel

You can also go to **Load Balance > Status** to see the status of FortiControllers (both slot icons should be green because both FortiControllers process traffic).



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.



Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

Make sure the FortiController fabric backplane ports are set to the correct

To change backplane fabric channel interface speeds, from the GUI go to **Switch > Fabric Channel** and edit the slot-3, slot-4, and slot-5 interface. Set the Speed to

speed. Since the workers are FortiGate-5001Ds and the cluster is using FortiGate-5144C chassis, the FortiController fabric backplane interface speed should be set to 40Gbps full duplex.

40Gbps Full-duplex and select OK.

From the CLI enter the following command to change the speed of the slot-4 port.

```
config switch fabric-channel physical-port
  edit slot-3
    set speed 40000full
  next
  edit slot-4
    set speed 40000full
  next
  edit slot-5
    set speed 40000full
  end
end
```

You can also enter this command to set the External Management IP and configure management access:

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers. The CLI syntax shows setting the default base management VLAN (101). You can use this command to change the base management VLAN.

```
config load-balance setting
  config base-mgmt-interfaces
    edit b1
      set vlan-id 101
    next
    edit b2
      set vlan-id 101
    end
  end
```

Enable base control traffic between FortiControllers. The CLI syntax shows setting the default base control VLAN (301). You can use this command to change the base management VLAN.

```
config load-balance setting
  config base-ctrl-interfaces
    edit b1
      set vlan-id 301
    next
    edit b2
      set vlan-id 301
    end
  end
```

# 7. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. This will reset the worker to factory default settings.

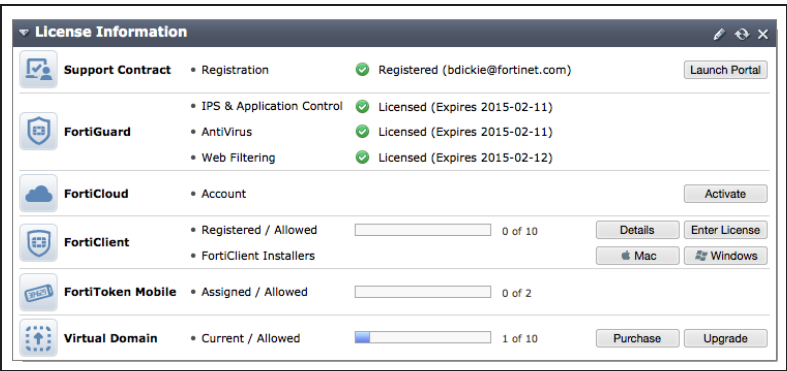
Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
  edit mgmt1
    set ip 172.20.120.120
  end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
  set hostname worker-chassis-1-slot-3
end
```

Register each worker and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You can also install any third-party certificates on the primary worker before forming the cluster. Once the cluster is formed, third-party certificates are synchronized to all of the workers.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
  set mode dual-forticontroller
end
```

Set the backplane communication speed of the workers to 40Gbps to match the FortiController-5903C.

```
config system interface
  edit elbc-ctrl/1
    set speed 40000full
  next
  edit elbc-ctrl/2
    set speed 40000full
end
```

## 8. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP. You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiControllers. The special port number begins with the standard port number for the protocol you are using and is followed by two digits that identify the chassis number and slot number. The port number is determined using the following formula:

**service\_port x 100 + (chassis\_id - 1) x 20 + slot\_id**

**service\_port** is the normal port number for the management service (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP). **chassis\_id** is the Chassis ID part of the FortiController HA configuration and can be 1 or 2. **slot\_id** is the number of the chassis slot.

Some examples:

- HTTPS, chassis 1 slot 2:  $443 \times 100 + (1 - 1) \times 20 + 2 = 44300 + 0 + 2 = 44302$ , browse to: <https://172.20.120.100:44302>
- HTTP, chassis 2, slot 4:  $80 \times 100 + (2 - 1) \times 20 + 4 = 8000 + 20 + 4 = 8024$ , browse to: <http://172.20.120.100/8024>
- HTTPS, chassis 1, slot 10:  $443 \times 100 + (1 - 1) \times 20 + 10 = 44300 + 0 + 10 = 44310$ , browse to <https://172.20.120.100/44330>
- HTTPS, chassis 2, slot 10:  $443 \times 100 + (2 - 1) \times 20 + 10 = 44300 + 20 + 10 = 44330$ , browse to <https://172.20.120.100/44330>
- SNMP query port, chassis 1, slot 4:  $161 \times 100 + (1 - 1) \times (20 + 4) = 16100 + 0 + 4 = 16104$

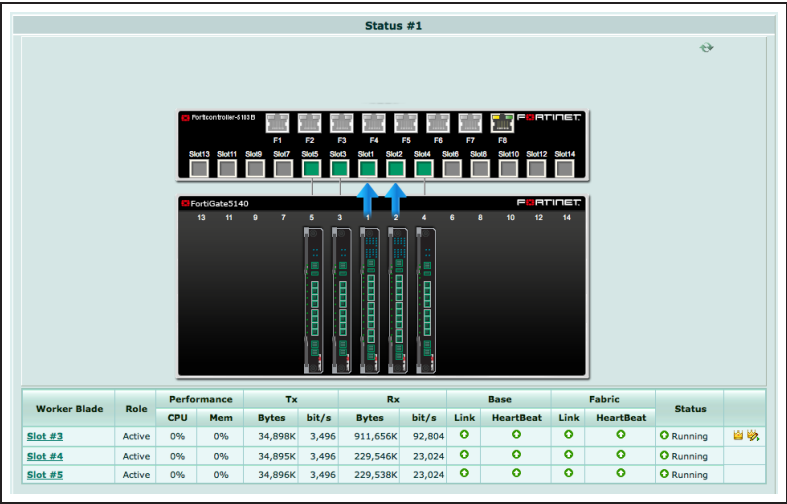
- Telnet to connect to the CLI of the worker in chassis 2 slot 4: telnet 172.20.120.100 2324
- To use SSH to connect to the CLI the worker in chassis 1 slot 5: ssh admin@172.20.120.100 -p2205

You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiControllers is by using its special port number (or a serial connection to the Console port).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

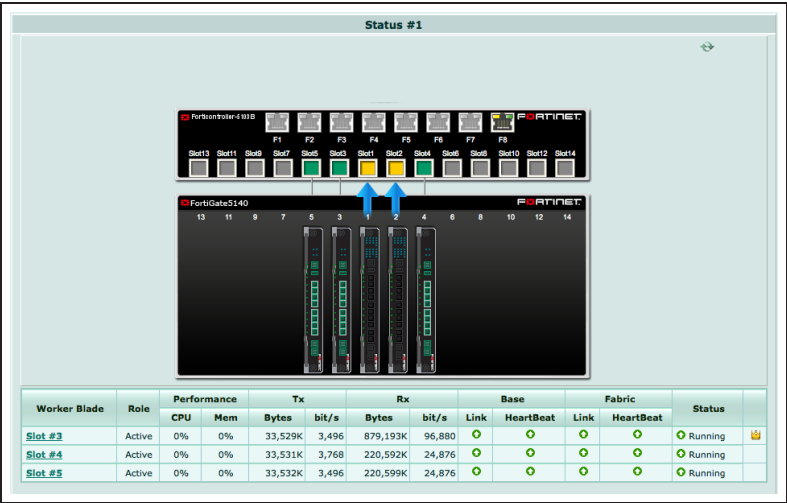
On the primary FortiController GUI go to **Load Balance > Status**. If the workers in chassis 1 are configured correctly they should appear in their appropriate slots

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Log into a backup FortiController GUI (for example by browsing to <https://172.20.120.100:44321> to log into the FortiController in chassis 2 slot 1) and go to **Load Balance > Status**. If the workers in chassis 2 are configured correctly they should appear in their appropriate slots.

The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.





## 9. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 (fctrl1/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl2/f6) you can access the root VDOM and add a policy to allow users on the Internal network to access the Internet.

|                     |                 |   |
|---------------------|-----------------|---|
| Incoming Interface  | fctrl2/f3       | + |
| Source Address      | Internal_Net    | + |
| Source User(s)      | Click to add... |   |
| Source Device Type  | Click to add... |   |
| Outgoing Interface  | fctrl1/f1       | + |
| Destination Address | all             | + |
| Schedule            | always          |   |
| Service             | ALL             | + |
| Action              | ACCEPT          |   |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

## 10. Results - Primary FortiController cluster status

Log into the **primary FortiController CLI** and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2201
```

```
get system status
Versio: FortiController-5903C v5.0,build0024
14815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: dual, master
System time: Mon Sep 15 10:11:48 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot  3: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  4: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  5: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
```

```
Heartbeat: Management: Good    Data: Good
Status Message:"Running"
Heartbeat: Management: Good    Data: Good
Status Message:"Running"get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
Slot  3: Status:Working    Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good    Data: Good
  Status Message:"Running"
Slot  4: Status:Working    Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good    Data: Good
  Status Message:"Running"
Slot  5: Status:Working    Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good    Data: Good
  Status Message:"Running"
Heartbeat: Management: Good    Data: Good
Status Message:"Running"
```

Enter this command from the primary FortiController to show the HA status of the FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (in this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201,
uptime=1517.38, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203,
uptime=1490.50, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=82192.16 status=alive
                        local_interface=      b2 last_hb_time=      0.00 status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204,
uptime=1476.37, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=82192.27 status=alive
                        local_interface=      b2 last_hb_time=      0.00 status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202,
uptime=1504.58, chassis=1(1)
```

```

slot: 2
sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=        b1 last_hb_
time=82192.16    status=alive
                local_interface=        b2 last_hb_time=    0.00    status=dead

```

## 11. Results - Chassis 1 Slot 2 FortiController status

Log into the **chassis 1 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2202
```

```

get system status
Version: FortiController-5903C
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:14:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)

```

Enter this command to view the status of this backup FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot  3: Status:Working  Function:Active
    Link:      Base: Down    Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  4: Status:Working  Function:Active
    Link:      Base: Down    Fabric: Up

```

```

Heartbeat: Management: Good    Data: Good
Status Message:"Running"
Slot 5: Status:Working    Function:Active
Link:      Base: Down      Fabric: Up
Heartbeat: Management: Good    Data: Good
Status Message:"Running"

```

Enter this command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202,
uptime=1647.44, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 best=yes
      local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201,
uptime=1660.17, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=82305.93    status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203,
uptime=1633.27, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=82305.83    status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

```

```
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204,
uptime=1619.12, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=          b1 last_hb_
time=82305.93    status=alive
                  local_interface=          b2 last_hb_time=    0.00    status=dead
```

## 12. Results - Chassis 2 Slot 1 FortiController status

Log into the **chassis 2 slot 1 FortiController** CLI and enter this command to view the status of this backup FortiController:

To use SSH:

```
ssh admin@172.20.120.100 -p2221

get system status
Version: FortiController-5903C
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: dual, backup
System time: Mon Sep 15 10:17:10 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada))
```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot 3: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
```

```

    Status Message:"Running"
Slot 4: Status:Working    Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good    Data: Good
Status Message:"Running"
Slot 5: Status:Working    Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good    Data: Good
Status Message:"Running"

```

Enter this command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203,
uptime=1785.61, chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=        b1 best=yes
        local_interface=        b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201,
uptime=1812.38, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=        b1 last_hb_
time=79145.95    status=alive
        local_interface=        b2 last_hb_time=        0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204,
uptime=1771.36, chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=        b1 last_hb_
time=79145.99    status=alive

```



```

        local_interface=          b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202,
uptime=1799.56, chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=          b1 last_hb_
time=79145.86    status=alive
        local_interface=          b2 last_hb_time=      0.00    status=dead

```

### 13. Results - Chassis 2 Slot 2 FortiController status

Log into the **chassis 2 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2222
```

```

get system status
Version: FortiController-5903C
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:20:00 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

Enter this command to view the status of the backup FortiController and its workers.

```

get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: N/A
  Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]
    Slot  3: Status:Working  Function:Active

```

```

Link:      Base: Down      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 4: Status:Working  Function:Active
Link:      Base: Down      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 5: Status:Working  Function:Active
Link:      Base: Down      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

```

Enter this command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot2 (FT513B3913000168), Slave(priority=3), ip=169.254.128.204,
uptime=1874.39, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch1-slot1 (FT513B3912000029), Master(priority=0), ip=169.254.128.201,
uptime=1915.59, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 last_hb_
time=78273.86  status=alive
                        local_interface=      b2 last_hb_time=      0.00  status=dead

ch2-slot1 (FT513B3912000051), Slave(priority=2), ip=169.254.128.203,
uptime=1888.78, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0

```

```

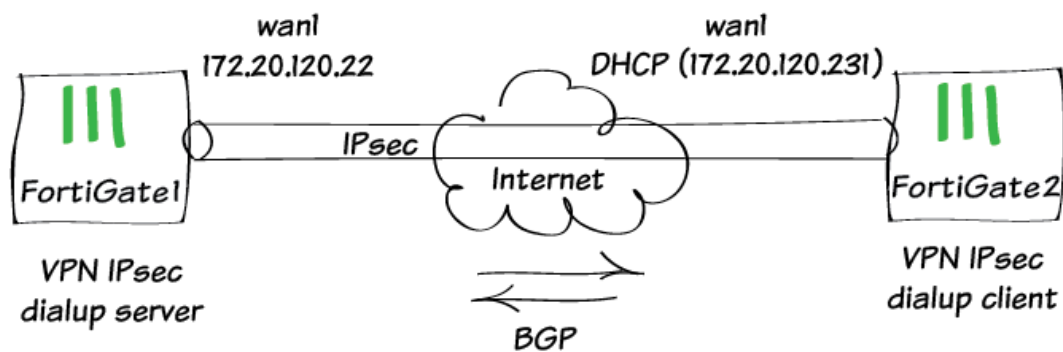
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=78273.85    status=alive
                local_interface=      b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202,
uptime=1902.72, chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_
time=78273.72    status=alive
                local_interface=      b2 last_hb_time=      0.00    status=dead

```

For further reading, check out the  
**FortiController Session-aware Load  
Balancing Guide.**

# BGP over a dynamic IPsec VPN



This example shows how to create a dynamic IPsec VPN tunnel and allowing BGP peering through it.

# 1. Configuring IPsec in FortiGate 1

Go to **Policy & Objects > Objects > Addresses** and select create new **Address**.

Then create **Address Group**.

Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-  
interface  
    edit Dialup  
        set type dynamic  
        set interface wan1  
        set mode aggressive  
        set peertype one  
        set mode-cfg enable  
        set proposal 3des-  
sha1 aes128-sha1  
        set peerid dial  
        set assign-ip  
disable  
        set psksecret  
    next  
end
```

Create phase 2.

```
config vpn ipsec phase2-interface  
    edit dial_p2  
        set phase1name Dialup  
        set proposal 3des-sha1 aes128-  
sha1  
        set src-addr-type name  
        set dst-addr-type name  
        set src-name all  
        set dst-name VPN_DST  
    next  
end
```

## 2. Configuring BGP in FortiGate 1

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```
config router bgp
  set as 100
  set router-id 1.1.1.1
  config neighbor
    edit 10.10.10.10
      set ebgp-enforce-
multihop enable
      set remote-as 200
      set update-source loop
    next
  end
  config redistribute connected
    set status enable
  end
end
```

## 3. Adding policies in FortiGate 1

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

## 4. Configuring IPsec in FortiGate 2

Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
  edit Dialup
    set interface wan1
    set mode aggressive
    set mode-cfg enable
    set proposal 3des-sha1 aes128-sha1
    set localid dial
    set remote-gw 172.20.120.22
    set assign-ip disable
    set psksecret
  next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
```

```

edit dial_p2
    set phase1name Dialup
    set proposal 3des-sha1 aes128-sha1
    set keepalive enable
next
end

```

## 5. Configuring BGP in FortiGate 2

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```

config router bgp
    set as 200
    set router-id 1.1.1.2
    config neighbor
        edit 20.20.20.20
            set ebgp-enforce-multihop enable
            set remote-as 100
            set update-source loopback
        next
    end
    config redistribute connected
        set status enable
    end
end

```

## 6. Adding policies in FortiGate 2

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

## 7. Adding a static route in FortiGate 2

Go to **Router > Static > Static Routes** and add a route to the remote Loopback interface via **Dialup** interface.

## 8. Verifying tunnel is Up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **Up**.

## 9. Results

From FortiGate 1, Go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via BGP.

From FortiGate 1, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.1, local
AS number 100
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries
Neighbor      V      AS MsgRcvd
MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd

10.10.10.10    4          200    8257
8237          7    0    0 5d00h01m
4
Total number of neighbors 1
```

From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via BGP.



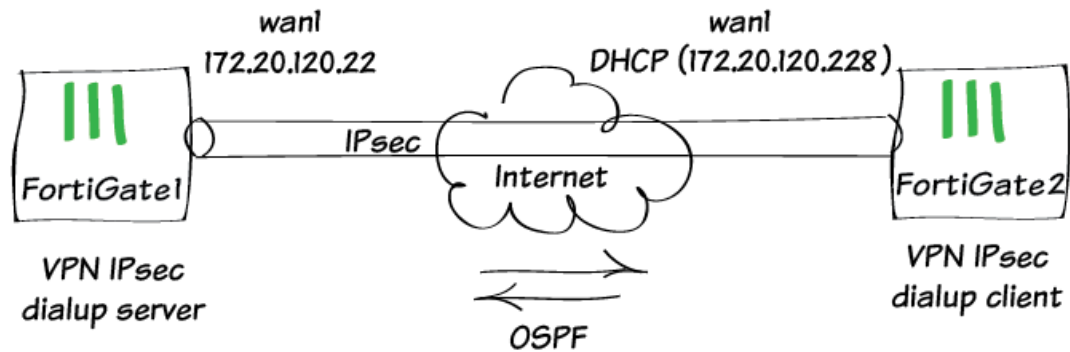
From FortiGate 2, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.2, local
AS number 200
BGP table version is 11
2 BGP AS-PATH entries
0 BGP community entries
Neighbor      V      AS MsgRcvd
MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd

20.20.20.20      4          100    8341
8361             10      0      0 5d01h32m
3
Total number of neighbors 1
```

For further reading, check out **IPsec VPN** and **Border Gateway Protocol (BGP)** in the **FortiOS 5.2 Handbook**.

# OSPF over dynamic IPsec VPN



This example shows how to create a dynamic IPsec VPN tunnel and allowing OSPF through it.

## 1. Configuring IPsec in FortiGate 1

Go to **System > Status** to look for the **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
edit "dial-up"
set type dynamic
set interface "wan1"
set mode-cfg enable
set proposal 3des-sha1
set add-route disable
set ipv4-start-ip 10.10.101.0
set ipv4-end-ip 10.10.101.255
set psksecret
next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
edit "dial-up-p2"
set phase1name "dial-up"
set proposal 3des-sha1 aes128-sha1
next
end
```

## 2. Configuring OSPF in FortiGate 1

Go to **System > Status** to look for the CLI Console widget and create OSPF route.

```
config router ospf
set router-id 172.20.120.22
config area
edit 0.0.0.0
next
end
config network
edit 1
set prefix 10.10.101.0 255.255.255.0
next
end
config redistribute "connected"
set status enable
end
config redistribute "static"
set status enable
end
end
```

## 3. Adding policies in FortiGate 1

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from dial-up to port5.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | dial-up         |
| Source Address      | ALL             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | port5           |
| Destination Address | ALL             |
| Schedule            | always          |
| Service             | OSPF            |
| Action              | ACCEPT          |

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from port5 to dial-up interfaces.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | port5           |
| Source Address      | ALL             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | dial-up         |
| Destination Address | ALL             |
| Schedule            | always          |
| Service             | OSPF            |
| Action              | ACCEPT          |

## 4. Configuring IPSec in FortiGate 2

Go to **System > Status** to look for the **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
edit "dial-up-client"
set interface "wan1"
set mode-cfg enable
set proposal 3des-sha1
set add-route disable
set remote-gw 172.20.120.22
set psksecret
next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
edit "dial-up-client-p2"
set phasename "dial-up-client"
set proposal 3des-sha1 aes128-sha1
set auto-negotiate enable
next
end
```






## 5. Configuring OSPF in FortiGate 2

Go to **System > Status** to look for the **CLI Console** widget and create OSPF route.

```
config router ospf
  set router-id 172.20.120.25
  config area
    edit 0.0.0.0
    next
  end
  config network
    edit 1
    set prefix 10.10.101.0 255.255.255.0
    next
  end
  config redistribute "connected"
    set status enable
  end
  config redistribute "static"
    set status enable
  end
end
```

## 6. Adding policies in FortiGate 2

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from dial-up-client to port5.

|                     |  |
|---------------------|--|
| Incoming Interface  | dial-up-client   |
| Source Address      |  all      |
| Source User(s)      | Click to add...  |
| Source Device Type  | Click to add...  |
| Outgoing Interface  | port5  |
| Destination Address |  all    |
| Schedule            |  always |
| Service             |  OSPF   |
| Action              |  ACCEPT |

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing OSPF traffic from port5 to dial-up-client interfaces.

|                     |                 |
|---------------------|-----------------|
| Incoming Interface  | port5           |
| Source Address      | all             |
| Source User(s)      | Click to add... |
| Source Device Type  | Click to add... |
| Outgoing Interface  | dial-up-client  |
| Destination Address | all             |
| Schedule            | always          |
| Service             | OSPF            |
| Action              | ACCEPT          |

8. Verifying tunnel is up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is Up.

| Name           | Remote Gateway | Status | Incoming Data | Outgoing Data | Phase 2 Selectors |
|----------------|----------------|--------|---------------|---------------|-------------------|
| dial-up-client | 172.20.120.22  | Up     | 67.37 KB      | 26.81 KB      | dial-up-client-p2 |

9. Results

From FortiGate 1, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via OSPF.

| Type      | Network          | Gateway      | Interface | Up Time    | Distance | Metric |
|-----------|------------------|--------------|-----------|------------|----------|--------|
| Static    | 0.0.0.0/0        | 172.20.120.2 | wan1      |            | 10       | 0      |
| OSPF      | 10.10.10.10/32   | 10.10.101.1  | dial-up_0 | 0 00:12:03 | 110      | 10     |
| OSPF      | 10.10.90.0/24    | 10.10.101.1  | dial-up_0 | 0 00:12:03 | 110      | 10     |
| Connected | 10.10.101.0/30   | 0.0.0.0      | dial-up_0 |            | 0        | 0      |
| Connected | 10.10.101.0/30   | 0.0.0.0      | dial-up_0 |            | 0        | 0      |
| Connected | 20.20.20.20/32   | 0.0.0.0      | loop      |            | 0        | 0      |
| Connected | 172.20.120.0/24  | 0.0.0.0      | wan1      |            | 0        | 0      |
| Static    | 192.168.1.0/24   | 0.0.0.0      | To_home   |            | 5        | 0      |
| Connected | 192.168.100.0/24 | 0.0.0.0      | port5     |            | 0        | 0      |
| Connected | ::1/128          | ::           | root      |            | 0        | 0      |

From FortiGate 1, go to **System > Status** to look for the **CLI Console** widget and type this command to verify OSPF neighbors.

```
get router info ospf neighbor

OSPF process 0:
Neighbor ID Pri State Dead Time Address Interface
172.20.120.25 1 Full/ - 00:00:34 10.10.101.1
dial-up_0
```

From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via OSPF.

From FortiGate 2, go to **System > Status** to look for the **CLI Console** widget and type this command to verify OSPF neighbors.

```
get router info ospf neighbor
```

```
OSPF process 0:
```

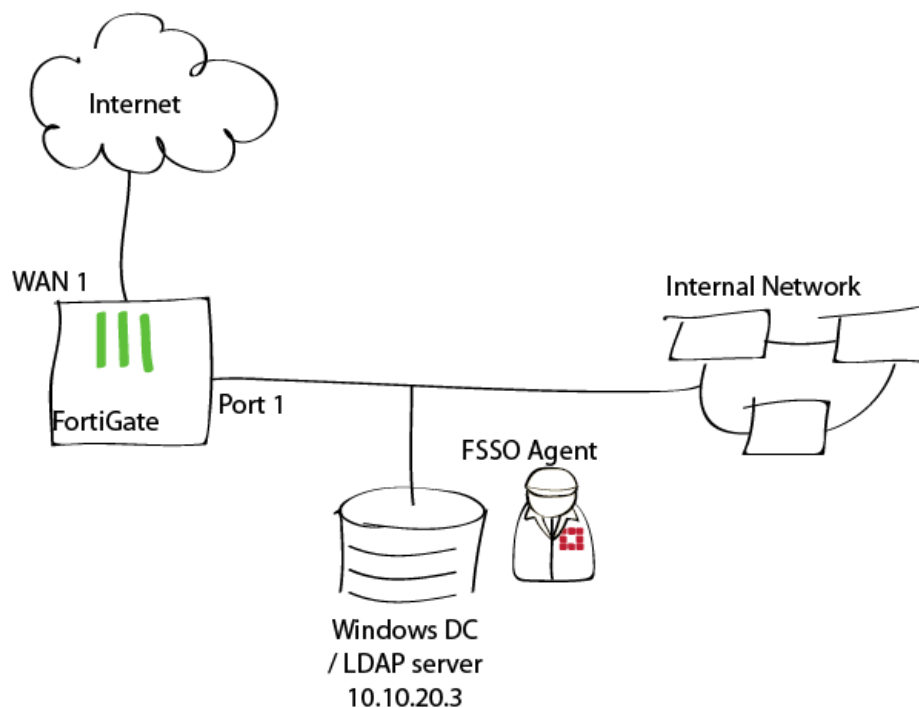
```
Neighbor ID Pri State Dead Time Address Interface  
172.20.120.22 1 Full/ - 00:00:30 10.10.101.2
```

```
dial-up-client
```

For further reading, check out [IPsec VPN](#) and [Open Shortest Path First \(OSPF\)](#) in the [FortiOS 5.2 Handbook](#).



# Single Sign-on using LDAP and FSSO agent in advanced mode



This recipe illustrates FortiGate user authentication with FSSO. In this example, user authentication controls Internet access and applies different security profiles for different users.

## 1. Integrating the FortiGate with the LDAP server

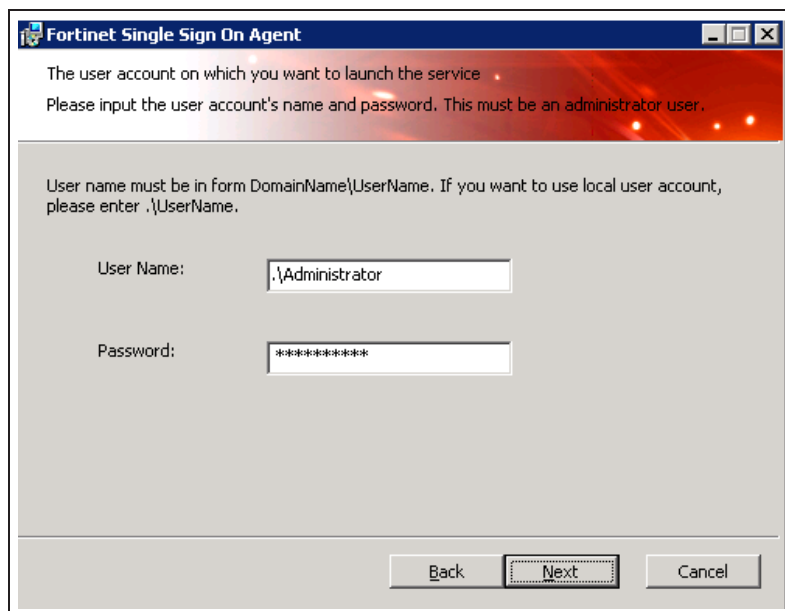
Go to **User & Device > Authentication > LDAP Servers** to configure the LDAP server.

|  |   |
|--|---|
| Name                                       | LDAP  |
| Server IP/Name                             | 10.10.20.3  |
| Server Port                                | 389   |
| Common Name Identifier                     | sAMAccountName  |
| Distinguished Name                         | dc=techdoc,dc=local   |
|  | <b>Fetch DN</b>   |
| Bind Type                                  | <input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular |
| User DN                                    | administrator@techdoc.local   |
| Password                                   | ••••••••  |
| <input type="checkbox"/> Secure Connection |   |

## 2. Installing FSSO agent on Windows AD server

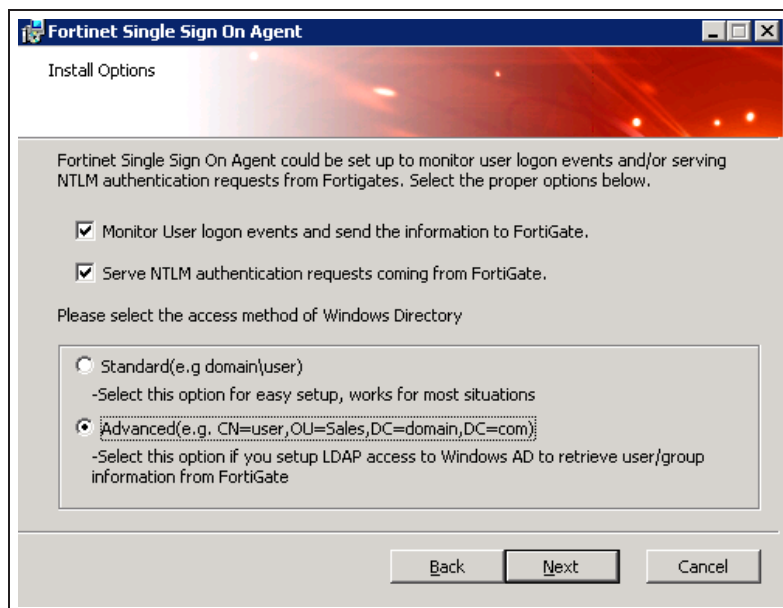
Accept the license and follow the Wizard.

Enter the Windows AD administrator password.

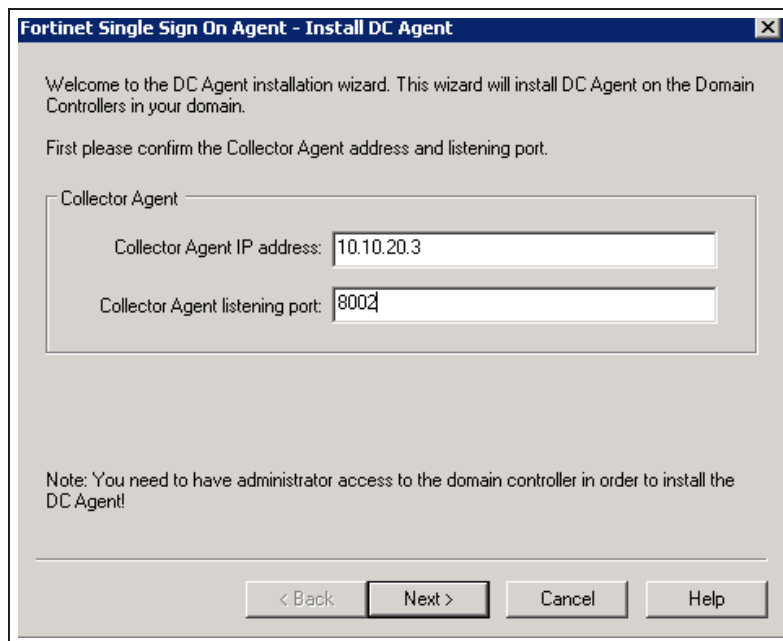


The screenshot shows the 'Fortinet Single Sign On Agent' installation wizard. The title bar is blue with the Fortinet logo and the text 'Fortinet Single Sign On Agent'. The main window has a red header bar with white text that reads: 'The user account on which you want to launch the service' and 'Please input the user account's name and password. This must be an administrator user.' Below this, a grey box contains the instruction: 'User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName.' There are two input fields: 'User Name:' with the text '.\Administrator' and 'Password:' with masked characters '\*\*\*\*\*'. At the bottom, there are three buttons: 'Back', 'Next' (which is highlighted with a dashed border), and 'Cancel'.

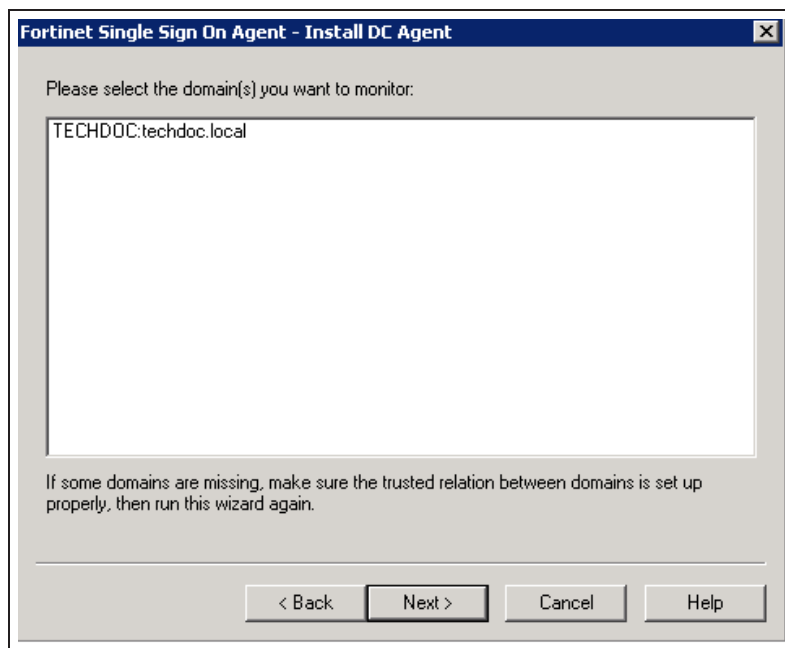
Select the **Advanced** Access method.



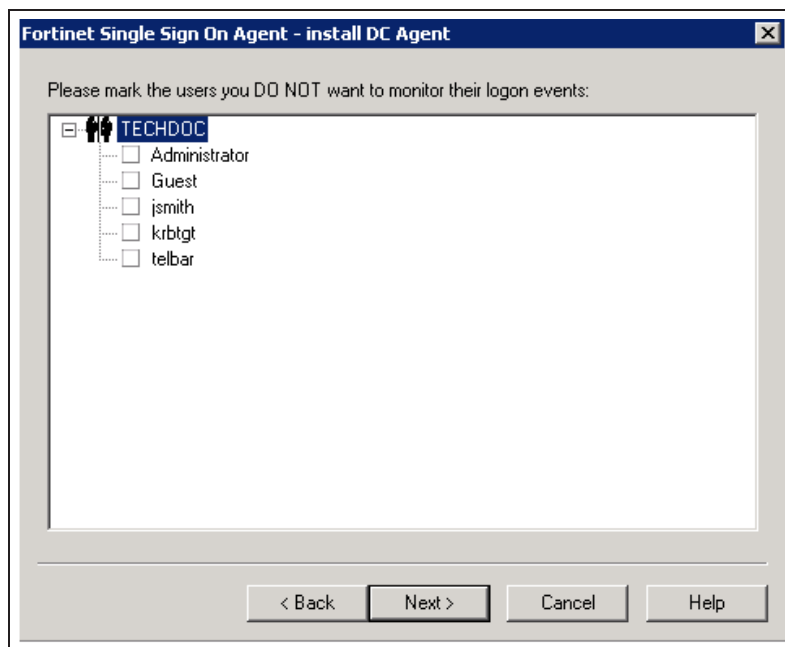
In the **Collector Agent IP address** field, enter the IP address of the Windows AD server.



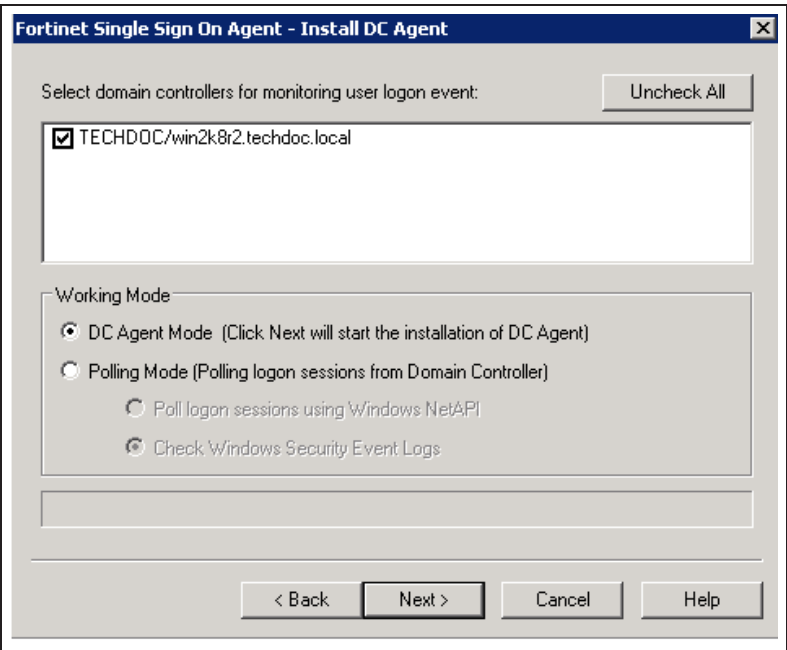
Select the domain you wish to monitor.



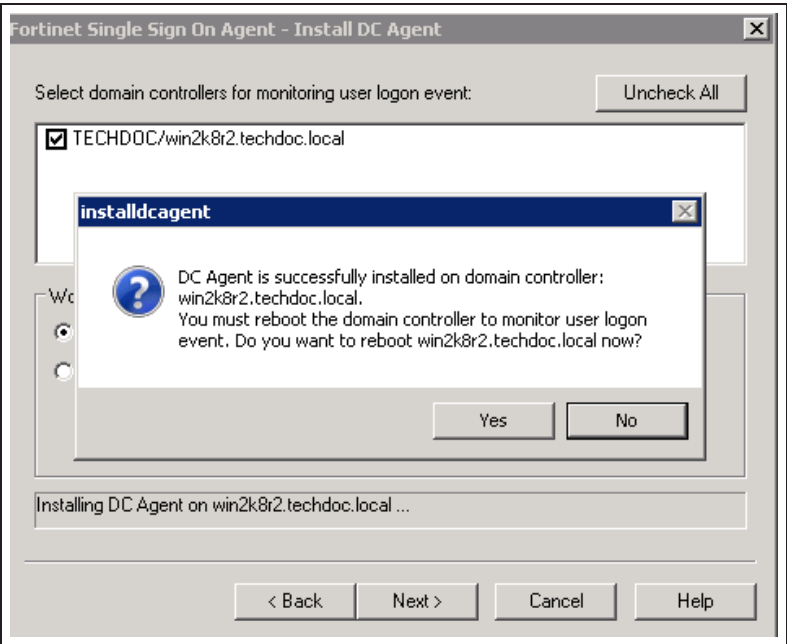
Next, select the users you do not wish to monitor.



Under **Working Mode**, select **DC Agent mode**.

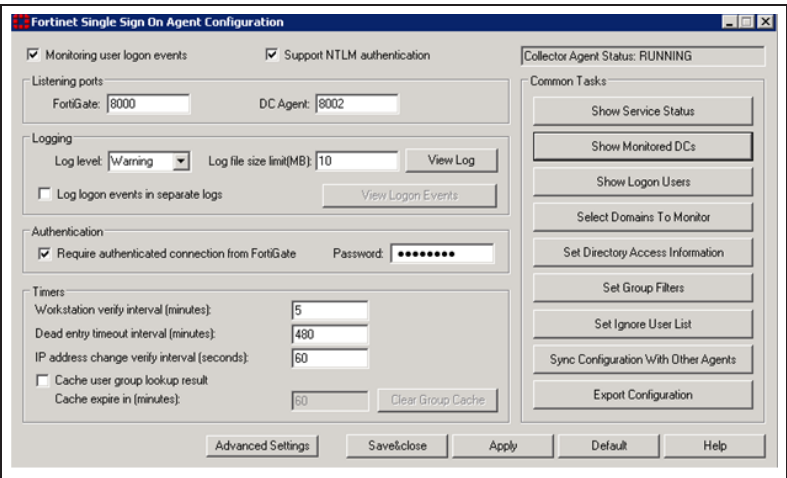


Reboot the Domain Controller.



Upon reboot, the collector agent will start up.

You can choose to **Require authenticated connection from FortiGate** and set a **Password**.

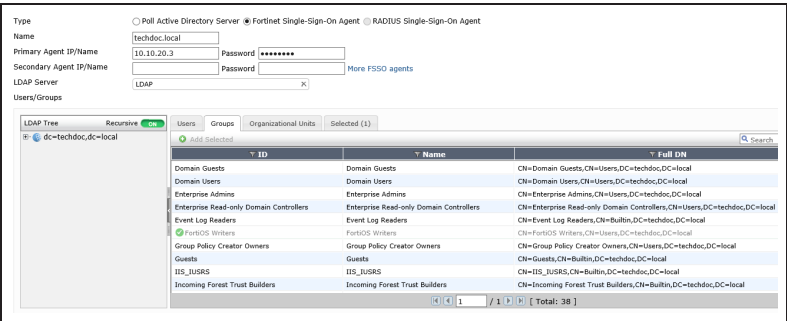


The screenshot shows the 'Fortinet Single Sign-On Agent Configuration' window. It has several sections: 'Monitoring user logon events' (checked), 'Support NTLM authentication' (checked), 'Listening ports' (FortiGate: 8000, DC Agent: 8002), 'Logging' (Log level: Warning, Log file size limit: 10 MB), 'Authentication' (Require authenticated connection from FortiGate: checked, Password: \*\*\*\*\*), and 'Timers' (Workstation verify interval: 5, Dead entry timeout interval: 480, IP address change verify interval: 60). On the right, there's a 'Collector Agent Status: RUNNING' and a 'Common Tasks' panel with buttons like 'Show Service Status', 'Show Monitored DCs', 'Show Logon Users', 'Select Domains To Monitor', 'Set Directory Access Information', 'Set Group Filters', 'Set Ignore User List', 'Sync Configuration With Other Agents', and 'Export Configuration'. At the bottom are buttons for 'Advanced Settings', 'Save/Close', 'Apply', 'Default', and 'Help'.

### 3. Configuring Single Sign-On on the FortiGate

Go to **User & Device > Authentication > Single Sign-On** and create a new SSO server.

Under **Groups** tab, select the user groups to be monitored. In this example, "FortiOS Writers" group is used.

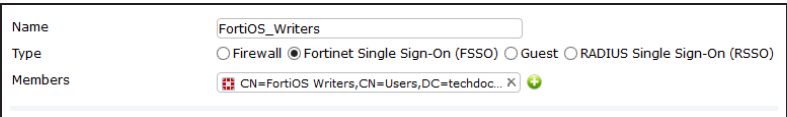


The screenshot shows the 'Single Sign-On' configuration window. It has tabs for 'Type', 'Users', 'Groups', and 'Organizational Units'. The 'Type' tab is selected, showing 'Poll Active Directory Server' (unchecked), 'Fortinet Single-Sign-On Agent' (checked), and 'RADIUS Single-Sign-On Agent' (unchecked). The 'Name' is 'techdoc.local', 'Primary Agent IP/Name' is '10.10.20.3', and 'Secondary Agent IP/Name' is empty. The 'LDAP Server' is 'LDAP'. The 'Users' tab is selected, showing a list of user groups. The 'FortiOS Writers' group is selected. The 'Groups' tab is also visible, showing a list of user groups. The 'Organizational Units' tab is also visible, showing a list of organizational units.

### 4. Creating a user group in the FortiGate

Go to **User & Device > User > User Groups** to create a new FSSO user group.

Under **Members**, select the "FortiOS\_Writers" group created earlier.



The screenshot shows the 'User Group' configuration window. It has fields for 'Name' (FortiOS\_Writers), 'Type' (Fortinet Single Sign-On (FSSO) selected), and 'Members' (CN=FortiOS Writers,CN=Users,DC=techdoc.local).

# 5. Adding a policy in the FortiGate

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing "FortiOS\_ writers" to navigate the Internet with appropriate security profiles.

default **Web Filter** security profile is used in this example.

|                     |                 |     |
|---------------------|-----------------|-----|
| Incoming Interface  | port1           | +   |
| Source Address      | all             | +   |
| Source User(s)      | FortiOS_Writers | x + |
| Source Device Type  | Click to add... |     |
| Outgoing Interface  | wan1            | +   |
| Destination Address | all             | +   |
| Schedule            | always          |     |
| Service             | ALL             | +   |
| Action              | ACCEPT          |     |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

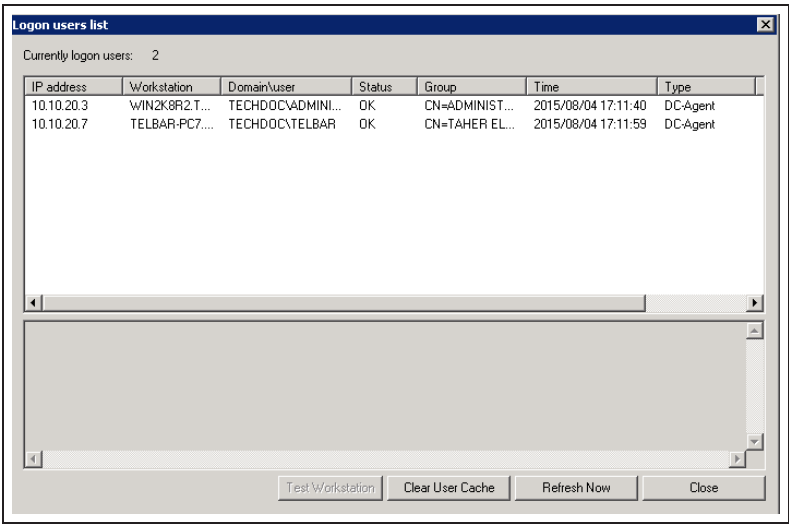
Click to add...

**Security Profiles**

|  |         |  |
|--|---------|--|
| <input type="checkbox"/> AntiVirus             | default |  |
| <input checked="" type="checkbox"/> Web Filter | default |  |
| <input type="checkbox"/> Application Control   | default |  |
| <input type="checkbox"/> IPS                   | default |  |
| <input type="checkbox"/> Email Filter          | default |  |
| <input type="checkbox"/> DLP Sensor            | default |  |

## 9. Results

Have users log on to the domain, go to the FSSO agent, and select **Show Logon Users**.



The screenshot shows a window titled "Logon users list" with a close button in the top right corner. Below the title bar, it says "Currently logon users: 2". There is a table with the following columns: IP address, Workstation, Domain\user, Status, Group, Time, and Type. Two rows of data are visible. Below the table is a large empty rectangular area with a scrollbar on the right. At the bottom of the window are four buttons: "Test Workstation", "Clear User Cache", "Refresh Now", and "Close".

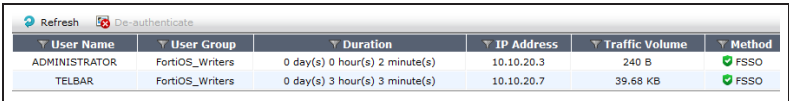
| IP address | Workstation    | Domain\user       | Status | Group          | Time                | Type     |
|------------|----------------|-------------------|--------|----------------|---------------------|----------|
| 10.10.20.3 | WIN2K8R2.T...  | TECHDOC\ADMINI... | OK     | CN=ADMINIST... | 2015/08/04 17:11:40 | DC-Agent |
| 10.10.20.7 | TELBAR-PC7.... | TECHDOC\TELBAR    | OK     | CN=TAHER EL... | 2015/08/04 17:11:59 | DC-Agent |

From the FortiGate, go to **System > Status** to look for the **CLI Console** widget and type this command for more detail about current FSSO logons:

diagnose debug authd fsso list

```
----FSSO logons----
IP: 10.10.20.3 User: ADMINISTRATOR Groups:
CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL
Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf:
FortiOS_Writers
IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS
WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation:
TELBAR-PC7.TECHDOC.LOCAL MemberOf: FortiOS_
Writers
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
```

From the FortiGate, go to **User & Device > Monitor > Firewall** and verify FSSO Logons.



The screenshot shows the "Firewall Monitor" page in the FortiGate GUI. At the top, there are "Refresh" and "De-authenticate" buttons. Below is a table with columns: User Name, User Group, Duration, IP Address, Traffic Volume, and Method. Two rows of data are shown, both for FSSO logons.

| User Name     | User Group      | Duration                       | IP Address | Traffic Volume | Method |
|---------------|-----------------|--------------------------------|------------|----------------|--------|
| ADMINISTRATOR | FortiOS_Writers | 0 day(s) 0 hour(s) 2 minute(s) | 10.10.20.3 | 240 B          | FSSO   |
| TELBAR        | FortiOS_Writers | 0 day(s) 3 hour(s) 3 minute(s) | 10.10.20.7 | 39.68 KB       | FSSO   |



Have users go to the Internet and the security profiles will be applied accordingly.

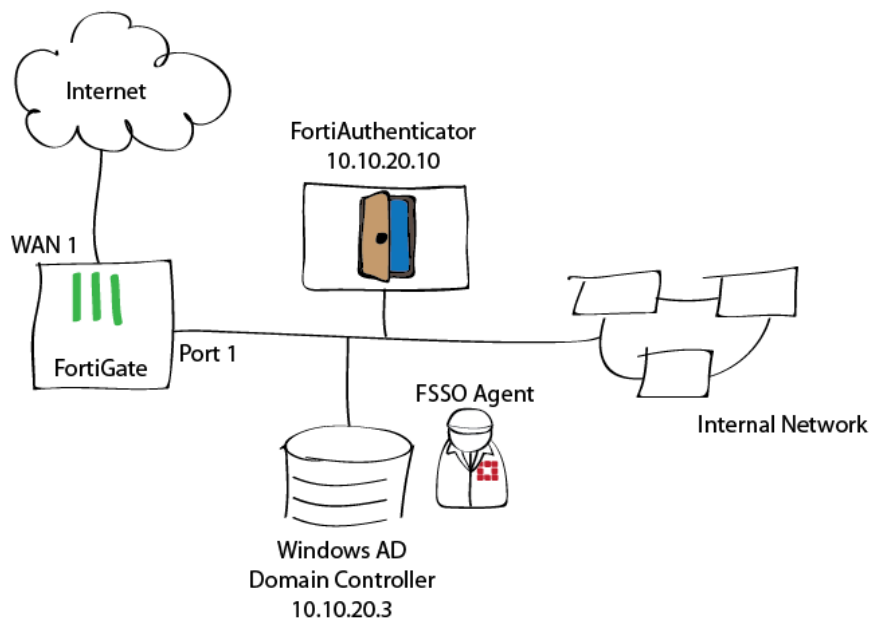
Go to **Log & Report > Traffic Log > Forward Traffic** to verify the log.

Select an entry for details.

| #  | @ | Date/Time | Source              | Destination                        | Application Name | Sent / Received     | Action | User   |
|----|---|-----------|---------------------|------------------------------------|------------------|---------------------|--------|--------|
| 1  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 1.38 KB / 4.70 KB   | close  | TELBAR |
| 2  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 2.45 KB / 10.38 KB  | close  | TELBAR |
| 3  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 2.43 KB / 59.94 KB  | close  | TELBAR |
| 4  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 7.51 KB / 126.59 KB | close  | TELBAR |
| 5  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 2.48 KB / 61.89 KB  | close  | TELBAR |
| 6  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 3.17 KB / 2.33 KB   | close  | TELBAR |
| 7  |   | 14:27:49  | TELBAR (10.10.20.7) | 208.91.114.176 (info.fortinet.com) | HTTPS            | 2.49 KB / 61.79 KB  | close  | TELBAR |
| 8  |   | 14:27:44  | TELBAR (10.10.20.7) | 134.170.21.245 (urs.microsoft.com) | HTTPS            | 2.33 KB / 7.00 KB   | close  | TELBAR |
| 9  |   | 14:27:44  | TELBAR (10.10.20.7) | 134.170.21.245 (urs.microsoft.com) | HTTPS            | 2.13 KB / 6.70 KB   | close  | TELBAR |
| 10 |   | 14:27:42  | 192.168.100.111     | 111.221.74.41                      | UDP/40005        | 173 B / 100 B       | accept |        |

|                     |                                      |                       |                                    |
|---------------------|--------------------------------------|-----------------------|------------------------------------|
| #                   | 1                                    | Action                | close                              |
| Date/Time           | 14:27:49                             | Destination           | 208.91.114.176 (info.fortinet.com) |
| Destination Country | United States                        | Destination Interface | wan1                               |
| Destination Port    | 443                                  | Duration              | 11                                 |
| Group               | FortiOS_Writers                      | Level                 | 4                                  |
| Log ID              | 13                                   | Policy ID             | 9                                  |
| Policy UUID         | 1014caf4-3541-51e5-8733-9d89455a30ff | Protocol              | tcp                                |
| Protocol Number     | 6                                    | Received Bytes        | 4701                               |
| Received Packets    | 10                                   | Sent Bytes            | 1377                               |
| Sent Packets        | 11                                   | Sequence Number       | 889674                             |
| Service             | HTTPS                                | Source                | TELBAR (10.10.20.7)                |
| Source Country      | Reserved                             | Source Interface      | port1                              |
| Source Port         | 52436                                | Src NAT IP            | 172.20.120.22                      |
| Src NAT Port        | 52436                                | Sub Type              | forward                            |
| Timestamp           | 8/4/2015, 2:27:49 PM                 | Tran Display          | snat                               |
| User                | TELBAR                               | Virtual Domain        | root                               |

# Single Sign-On using FSSO agent in advanced mode and FortiAuthenticator



This recipe demonstrates FortiGate user authentication with FSSO and the use of FortiAuthenticator as an LDAP server. In this example, user authentication controls Internet access and applies different security profiles for different users.

## 1. Configuring an LDAP directory on the FortiAuthenticator

Go to **Authentication > User Management > Local Users** to create a users list. Make sure to enable **Allow LDAP browsing**.

|   |  |
|---|--|
| Username:   | telbar   |
| <input type="checkbox"/> Disabled                                 |  |
| <input checked="" type="checkbox"/> Password-based authentication | <a href="#">[Change Password]</a>  |
| <input type="checkbox"/> Token-based authentication               |  |
| <input type="checkbox"/> Allow RADIUS authentication              |  |
| <input type="checkbox"/> Enable account expiration                |  |
| <b>User Role</b>  |  |
| Role:   | <input type="radio"/> Administrator<br><input checked="" type="radio"/> User |
| <input checked="" type="checkbox"/> Allow LDAP browsing           |  |
| ▶ User Information  |  |
| ▶ Alternative Email Addresses                                     |  |
| ▶ Password Recovery Options                                       |  |
| ▶ Groups  |  |
| ▶ Email Routing   |  |
| ▶ RADIUS Attributes   |  |
| ▶ Certificate Bindings  |  |

Go to **Authentication > User Management > User Groups** to create a user group and add users to it. "FortiOS\_Writers" user group is used in this example.

Name: FortiOS\_Writers

Type: ☒ Local ☐ Remote LDAP ☐ Remote RADIUS

Users:

Available users

Filter

test

Selected users

telbar

Choose all visible

Remove all

Go to **Authentication > LDAP Service > Directory tree** and configure the LDAP directory tree.

Expand All Delete (191 of 200 entries remaining)

dc=techdoc,dc=local (4)

cn=FortiOS\_Writers

ou=Cookbook (1)

uid=telbar

ou=FortiOS (2)

cn=Writers (1)

uid=telbar

uid=telbar

Use CTRL key to select multiple entries, or drag to move selected entries with your mouse

## 2. Integrating the FortiGate with the FortiAuthenticator

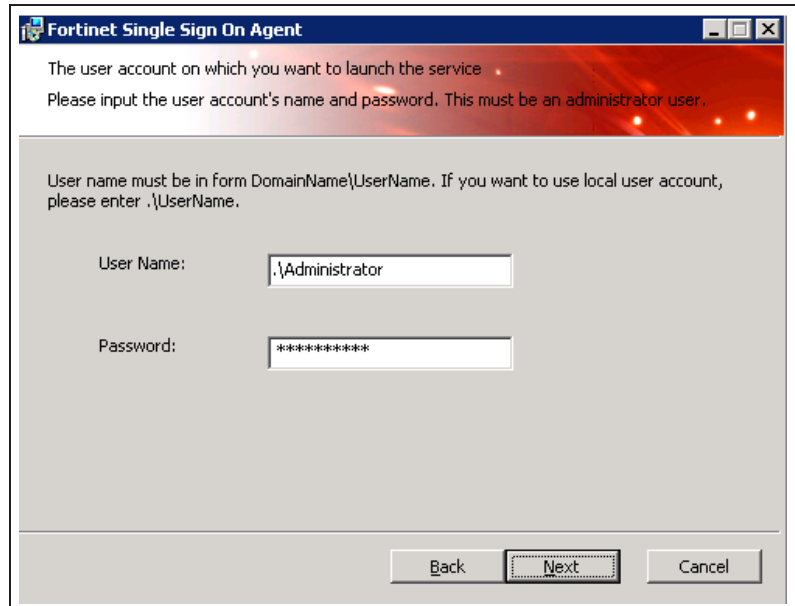
Go to **User & Device > Authentication > LDAP Servers** and configure the LDAP server.

|  |   |
|--|---|
| Name                                       | <input type="text" value="FAC_LDAP"/>   |
| Server IP/Name                             | <input type="text" value="10.10.20.10"/>  |
| Server Port                                | <input type="text" value="389"/>  |
| Common Name Identifier                     | <input type="text" value="uid"/>  |
| Distinguished Name                         | <input type="text" value="dc=techdoc,dc=local"/>  |
|  | <input type="button" value="Fetch DN"/>   |
| Bind Type                                  | <input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular |
| User DN                                    | <input type="text" value="uid=telbar,cn=Writers,ou=FortiOS,dc=techdoc,dc=local"/>                     |
| Password                                   | <input type="password" value="*****"/>  |
| <input type="checkbox"/> Secure Connection |   |

## 3. Installing the FSSO agent on the Windows AD server

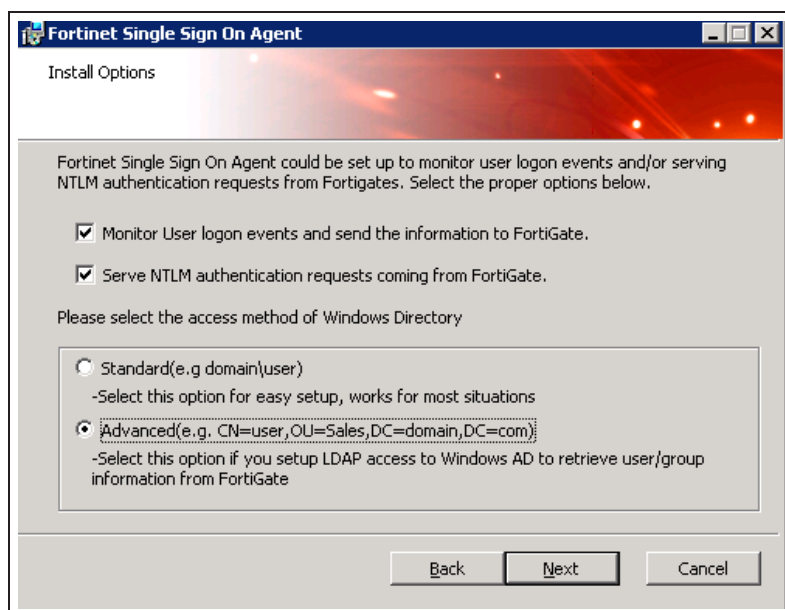
Accept the license and follow the Wizard.

Enter the Windows AD administrator password.

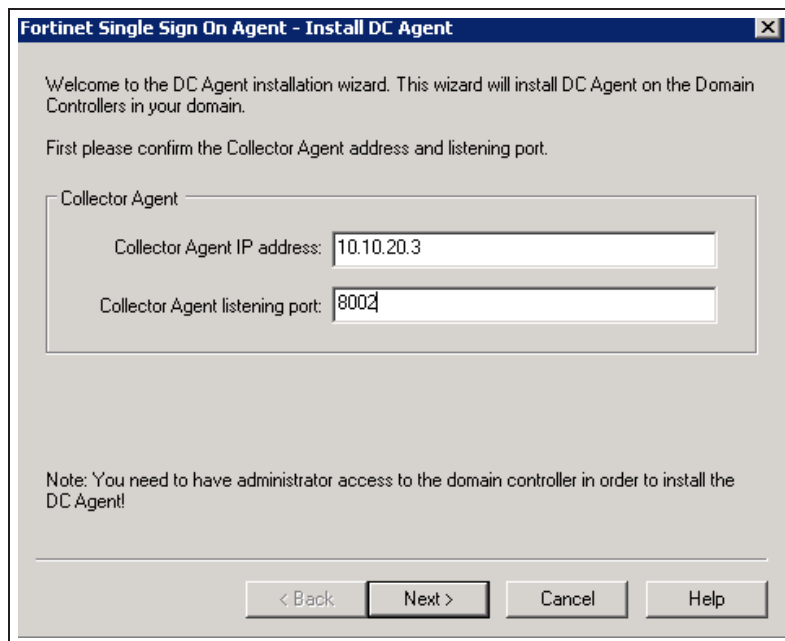


The window is titled "Fortinet Single Sign On Agent". It has a red header bar with the title. Below the header, there is a message: "The user account on which you want to launch the service". Below that, another message: "Please input the user account's name and password. This must be an administrator user." Below these messages, there is a text box for "User name" with the instruction: "User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName." The "User Name" field contains ".\Administrator". Below that is a "Password" field containing "\*\*\*\*\*". At the bottom right, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a dashed border.

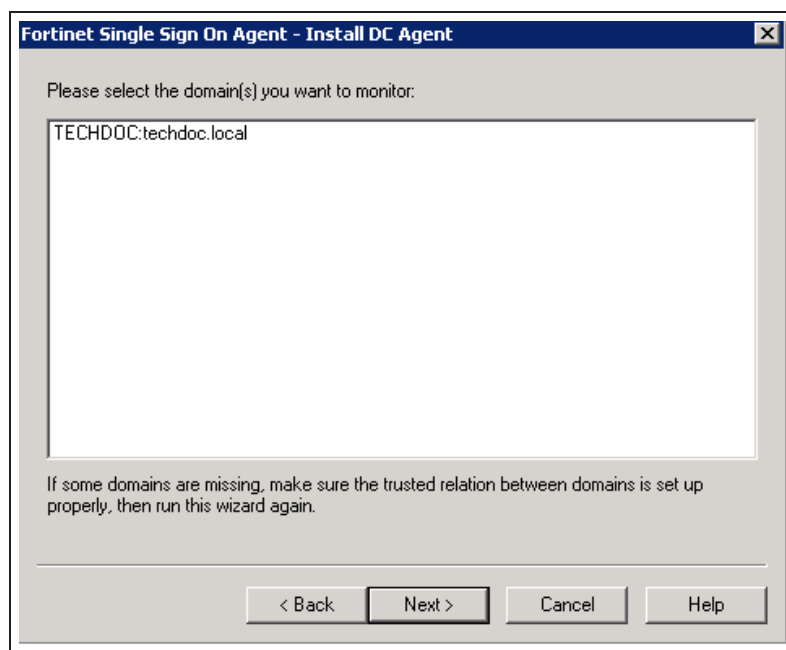
Select the **Advanced** Access method.



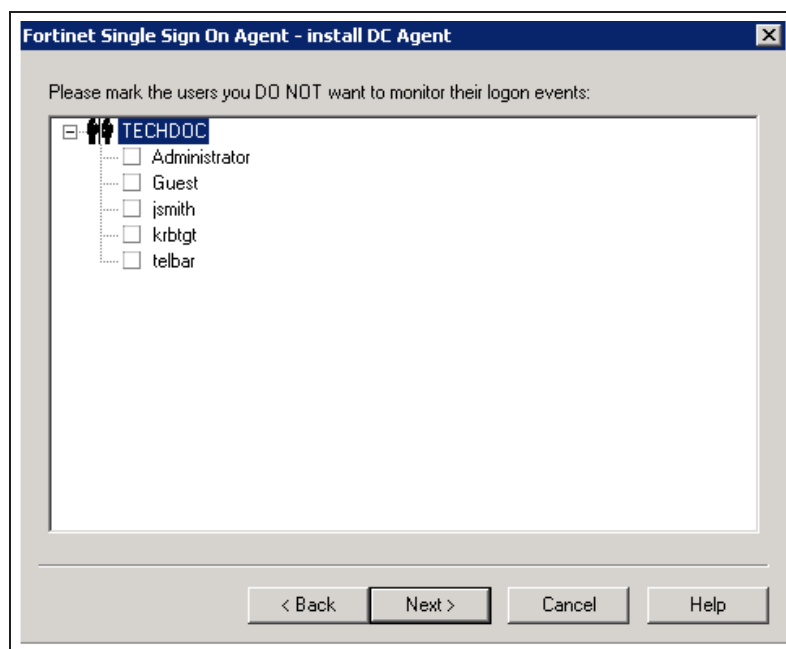
In the **Collector Agent IP address** field, enter the IP address of the Windows AD server.



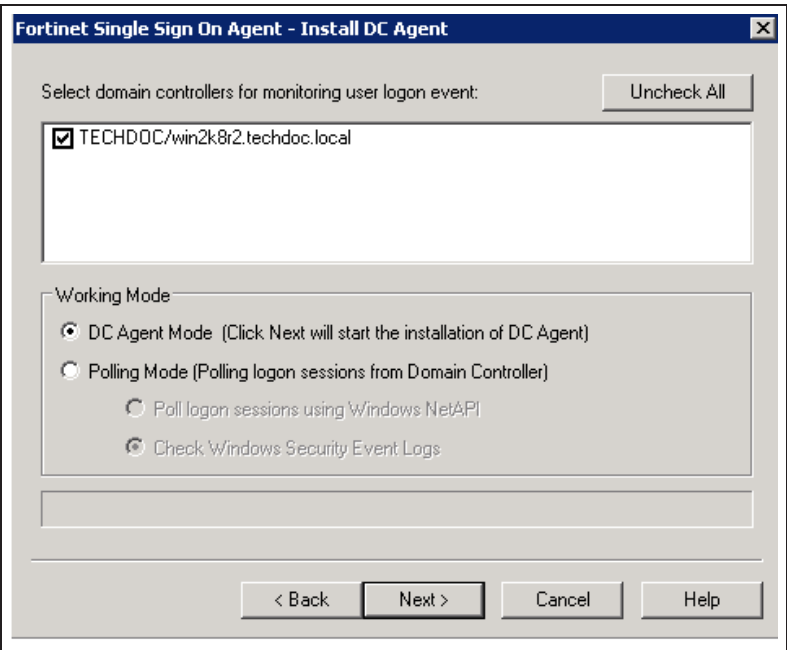
Select the domain you wish to monitor.



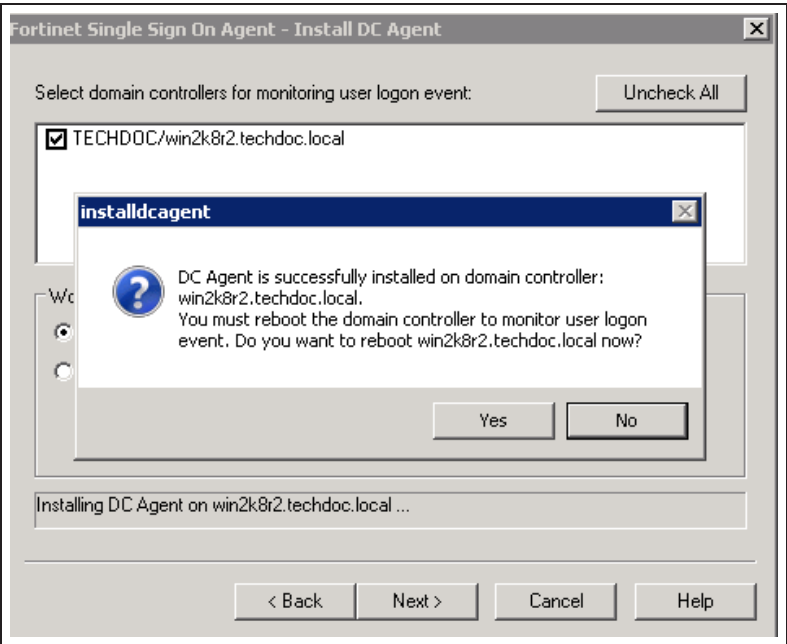
Next, select the users you do not wish to monitor.



Under **Working Mode**, select **DC Agent mode**.



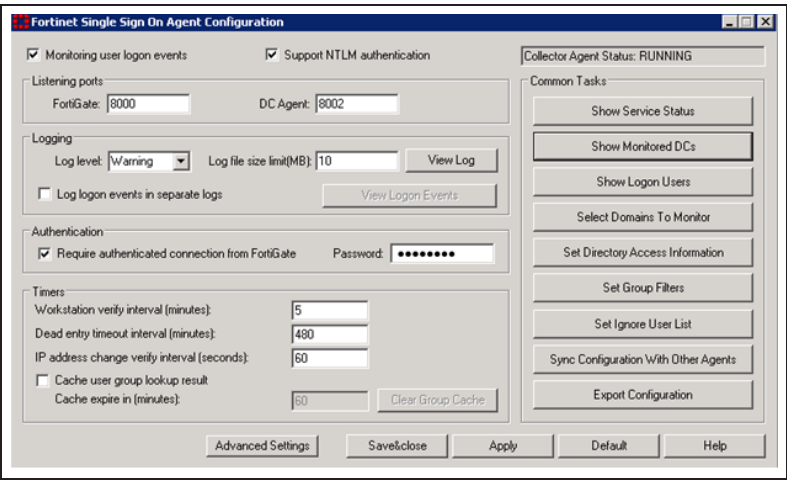
Reboot the Domain Controller.





Upon reboot, the collector agent will start up.

You can choose to **Require authenticated connection from FortiGate** and set a **Password**.

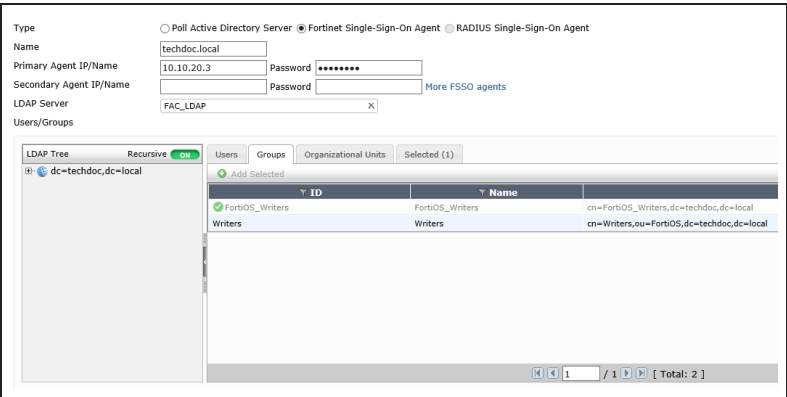


The screenshot shows the 'Fortinet Single Sign On Agent Configuration' window. It has several sections: 'Monitoring user login events' (checked), 'Support NTLM authentication' (checked), 'Listening ports' (FortiGate: 8000, DC Agent: 8002), 'Logging' (Log level: Warning, Log file size limit: 10 MB), 'Authentication' (Require authenticated connection from FortiGate: checked, Password: masked), and 'Timers' (Workstation verify interval: 5, Dead entry timeout interval: 480, IP address change verify interval: 60). On the right, there's a 'Collector Agent Status: RUNNING' and a 'Common Tasks' panel with buttons like 'Show Service Status', 'Show Monitored DCs', 'Show Login Users', 'Select Domains To Monitor', 'Set Directory Access Information', 'Set Group Filters', 'Set Ignore User List', 'Sync Configuration With Other Agents', and 'Export Configuration'. At the bottom are buttons for 'Advanced Settings', 'Save/Close', 'Apply', 'Default', and 'Help'.

## 4. Configuring Single Sign-On on the FortiGate

Go to **User & Device > Authentication > Single Sign-On** and create a new SSO server.

Under **Groups** tab, select the user groups to be monitored. In this example, "FortiOS\_Writers" group is used.



The screenshot shows the 'Single Sign-On' configuration page in FortiGate. It has tabs for 'Type', 'Name', 'Primary Agent IP/Name', 'Secondary Agent IP/Name', 'LDAP Server', and 'Users/Groups'. The 'Type' tab is selected, showing 'Poll Active Directory Server' (selected), 'Fortinet Single-Sign-On Agent', and 'RADIUS Single-Sign-On Agent'. The 'Name' field is 'techdoc.local'. The 'Primary Agent IP/Name' is '10.10.20.3' and the 'Secondary Agent IP/Name' is '10.10.20.3'. The 'LDAP Server' is 'FAC\_LDAP'. The 'Users/Groups' tab is selected, showing a table of user groups. The table has columns 'ID', 'Name', and 'Full Name'. The 'FortiOS\_Writers' group is selected, and its full name is 'cn=FortiOS\_Writers,dc=techdoc,dc=local'.

## 5. Creating a user group in the FortiGate

Go to **User & Device > User > User Groups** to create new user group. Under **Remote groups**, add the remote LDAP server created earlier in the FortiAuthenticator (in this example it's called "FAC\_LDAP").



The screenshot shows the 'User Groups' configuration page in FortiGate. It has tabs for 'Name', 'Type', 'Members', and 'Remote groups'. The 'Name' field is 'FortiOS\_Writers'. The 'Type' is 'Firewall' (selected). The 'Members' field is 'Click to add...'. The 'Remote groups' tab is selected, showing a table of remote groups. The table has columns 'Remote Server' and 'Group Name'. The 'FAC\_LDAP' group is listed, and its group name is 'cn=FortiOS\_Writers,dc=techdoc,dc=local'.

## 6. Adding a policy in the FortiGate

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing "FortiOS\_writers" to navigate the Internet with appropriate security profiles.

default **Web Filter** security profile is used in this example.

|                     |                 |     |
|---------------------|-----------------|-----|
| Incoming Interface  | port1           | +   |
| Source Address      | all             | +   |
| Source User(s)      | FortiOS_Writers | X + |
| Source Device Type  | Click to add... |     |
| Outgoing Interface  | wan1            | +   |
| Destination Address | all             | +   |
| Schedule            | always          |     |
| Service             | ALL             | +   |
| Action              | ACCEPT          |     |

**Firewall / Network Options**

☒ NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

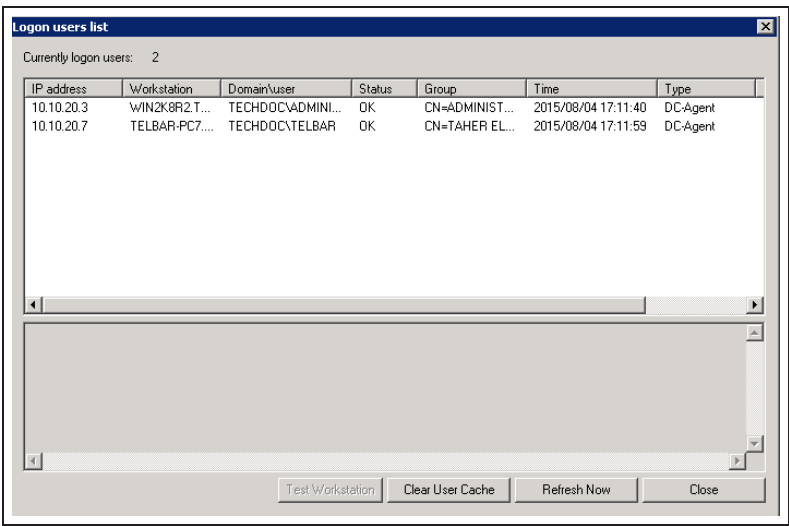
Click to add...

**Security Profiles**

|  |         |  |
|--|---------|--|
| <input type="checkbox"/> AntiVirus             | default |  |
| <input checked="" type="checkbox"/> Web Filter | default |  |
| <input type="checkbox"/> Application Control   | default |  |
| <input type="checkbox"/> IPS                   | default |  |
| <input type="checkbox"/> Email Filter          | default |  |
| <input type="checkbox"/> DLP Sensor            | default |  |

# 7. Results

Have users log on to the domain, go to the FSSO agent, and select **Show Logon Users**.



The screenshot shows a window titled "Logon users list" with a close button in the top right corner. Below the title bar, it says "Currently logon users: 2". There is a table with the following columns: IP address, Workstation, Domain\user, Status, Group, Time, and Type. Two rows of data are visible. Below the table is a large empty rectangular area with a scrollbar on the right. At the bottom of the window are four buttons: "Test Workstation", "Clear User Cache", "Refresh Now", and "Close".

| IP address | Workstation    | Domain\user       | Status | Group          | Time                | Type     |
|------------|----------------|-------------------|--------|----------------|---------------------|----------|
| 10.10.20.3 | WIN2K8R2.T...  | TECHDOC\ADMINI... | OK     | CN=ADMINIST... | 2015/08/04 17:11:40 | DC-Agent |
| 10.10.20.7 | TELBAR-PC7.... | TECHDOC\TELBAR    | OK     | CN=TAHER EL... | 2015/08/04 17:11:59 | DC-Agent |

From the FortiGate, go to **System > Status** to look for the **CLI Console** widget and type this command for more detail about current FSSO logons:

diagnose debug authd fsso list

----FSSO logons----

IP: 10.10.20.3 User: ADMINISTRATOR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf: FortiOS\_Writers  
IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: TELBAR-PC7.TECHDOC.LOCAL MemberOf: FortiOS\_Writers  
Total number of logons listed: 2, filtered: 0  
----end of FSSO logons----

Have users belonging to the "FortiOS\_Writes" user group navigate the Internet. An authentication portal is presented to allow only authorized users. Security profiles will be applied accordingly.




## Authentication Required

Please enter your username and password to continue.








Username:

Password:





Upon successful authentication, from the FortiGate, go to **User & Device > Monitor > Firewall** and verify FSSO Logons.

| User Name | User Group      | IP Address | Traffic Volume | Method   |
|-----------|-----------------|------------|----------------|--|
| telbar    | FortiOS_Writers | 10.10.20.7 | 2.99 MB        |  Firewall |

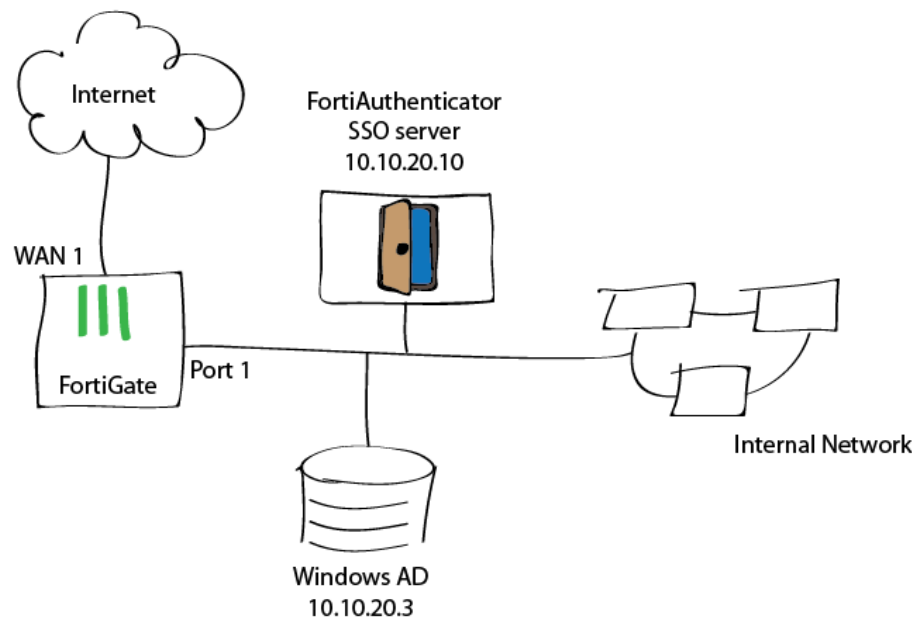
Go to **Log & Report > Traffic Log > Forward Traffic** to verify the log.

| #  | @ | Date/Time | Source  | Destination   | Application Name | Sent / Received    |
|----|---|-----------|---|---|------------------|--------------------|
| 7  |   | 09:59:48  |  telbar (10.10.20.7) |  184.106.91.131                        | HTTP             | 1.16 KB / 287 B    |
| 8  |   | 09:59:48  |  telbar (10.10.20.7) |  184.106.91.131                        | HTTP             | 2.16 B / 384 B     |
| 9  |   | 09:59:48  |  telbar (10.10.20.7) | 54.243.69.241 (ec2-54-243-69-241.compute-1.amazonaws.com)   | HTTP             | 860 B / 385 B      |
| 10 |   | 09:59:47  | 192.168.100.111   | 216.58.216.238 (www.google-analytics.com)   | HTTPS            | 10.49 KB / 6.96 KB |
| 11 |   | 09:59:41  | 192.168.100.111   |  208.91.114.47 (cookbook.fortinet.com) | HTTP             | 2.16 KB / 845 B    |
| 12 |   | 09:59:40  | 192.168.100.111   | 111.221.77.141  | UDP/40027        | 184 B / 118 B      |
| 13 |   | 09:59:40  | 192.168.100.111   |  111.221.77.173                      | UDP/40024        | 195 B / 80 B       |

Select an entry for details.

|                     |  |                       |   |
|---------------------|--|-----------------------|---|
| #                   | 7  | Action                | close   |
| Date/Time           | 09:59:48   | Destination           |  184.106.91.131      |
| Destination Country | United States  | Destination Interface | wan1  |
| Destination Port    | 80   | Duration              | 6   |
| Group               | FortiOS_Writers  | Level                 |  10000               |
| Log ID              | 13   | Policy ID             | 9   |
| Policy UUID         | 1014caf4-3541-51e5-8733-9d89455a30ff   | Protocol              | tcp   |
| Protocol Number     | 6  | Received Bytes        | 287   |
| Received Packets    | 5  | Sent Bytes            | 1161  |
| Sent Packets        | 5  | Sequence Number       | 748411  |
| Service             | HTTP   | Source                |  telbar (10.10.20.7) |
| Source Country      | Reserved   | Source Interface      | port1   |
| Source Port         | 51187  | Src NAT IP            | 172.20.120.22   |
| Src NAT Port        | 51187  | Sub Type              | forward   |
| Timestamp           | 8/17/2015 9:59:48 AM   | Tran Display          | snat  |
| User                |  telbar | Virtual Domain        | root  |

# SSO using a FortiGate, FortiAuthenticator, and DC Polling



This recipe demonstrates FortiGate user authentication with the use of a FortiAuthenticator as a Single Sign-On server. In this example, the FortiAuthenticator is configured to collect the user logon by polling the Domain Controller logs. User authentication controls Internet access and applies different security profiles for different users.

# 1. Configuring the FortiAuthenticator

Go to **Fortinet SSO Methods > SSO > General** to configure general settings as shown in the exhibit.

FortiGate

Listening port:

8000

☒ Enable authentication

Secret key:

.....

Login expiry:

480

minutes

Extend user session beyond logoff by:

0

seconds (0-3600)

☒ Enable NTLM authentication

User domain:

techdoc.local

Fortinet Single Sign-On (FSSO)

Maximum concurrent user sessions:

0

[\[Configure Per User/Group\]](#)

Log level:

Info

[\[Configure Log Filter\]](#)

☒ Enable Windows Active Directory domain controller polling

☒ Enable polling additional logon events

Additional logon event timeout:

480

minutes (1-7200)

☒ Enable DNS lookup to get IP from workstation name

☐ Directly use domain DNS suffix in lookup

☒ Enable reverse DNS lookup to get workstation name from IP

☒ Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name

☒ Include account name ending with \$ (usually computer account)

Go to **Fortinet SSO Methods > SSO > Domain Controllers** and add the Windows AD to the FortiAuthenticator.

NetBIOS name:

techdoc

Display name:

techdoc-WinAD

Domain controller IP:

10.10.20.3

Account:

Administrator

Password:

.....

Priority:

Primary

Go to **Authentication > Remote Auth. Servers > LDAP** to set the Windows AD as an LDAP server. This will be useful to import **SSO Filtering Objects** from Windows AD to the FortiAuthenticator.

|   |   |   |
|---|---|---|
| Name:   | WinLDAP   |   |
| Primary server name/IP:                       | 10.10.20.3  | Port: 389   |
| <input type="checkbox"/> Use secondary server |   |   |
| Base distinguished name:                      | DC=techdoc,DC=local   |   |
| Bind type:                                    | <input type="radio"/> Simple <input checked="" type="radio"/> Regular |   |
| Username:                                     | administrator@techdoc.local   | Password: .....                                       |
| User object class:                            | person  |   |
| Username attribute:                           | sAMAccountName  |   |
| Group object class:                           | group   |   |
| Group membership attribute:                   | memberOf  | <input type="checkbox"/> Attribute is group attribute |

Go to **Fortinet SSO Methods > SSO > FortiGate Filtering** and create a new FortiGate Filtering.

Under **Fortinet Single Sign-On (FSSO)**, enable **Forward FSSO** information for users from the following subset of users/groups/containers only.

Under **SSO Filtering Objects**, select **Import**, in the **Remote LDAP Server** field, select the LDAP server created earlier in the previous step (WinLDAP in this example) and select **Apply**.

Next, select groups or containers to be imported, controlled and monitored by the FortiAuthenticator. In this example the "FortiOS Writers" user group is selected.

Name: SSO-Filter

FortiGate name/IP: 10.10.20.1

Description:

IP Filtering

☐ Enable IP filtering for this service

Fortinet Single Sign-On (FSSO)

☒ Forward FSSO information for users from the following subset

SSO Filtering Objects

Create New

Import

Edit FortiGate Filter

Import Remote LDAP Objects - Mozilla Firefox

https://10.10.20.10/fose/import\_filtersbjs?\_gopage=1&client\_id=3

Import Remote LDAP Objects

Remote LDAP server: WinLDAP (10.10.20.3) Apply

Select users, groups or containers to import below:

A container has 3 modes to choose from:

- User container: users and future users in the selected container (and sub-containers) will be included in the filter.
- Group container: groups and future groups in the selected container (and sub-containers) will be included in the filter.
- User & group container: both users and groups and future users and groups in the selected container (and sub-containers) will be included in the filter.

DC=techdoc,DC=local

Cti-Computers container

Cti-Domain Controllers container

Cti-ForeignSecurityPrincipals container

Cti-Managed Service Accounts container

Cti-Program Data container

Cti-System container

Cti-Users container

Cti-administrator user

Cti-Allowed RODC Password Replication Group group

Cti-Cert Publishers group

Cti-Denied RODC Password Replication Group group

Cti-DiskAdmins group

Cti-OnsUpdateProxy group

Cti-Domain Admins group

Cti-Domain Computers group

Cti-Domain Controllers group

Cti-Domain Guests group

Cti-Domain Users group

Cti-Enterprise Admins group

Cti-Enterprise Read-only Domain Controllers group

Cti-FortiOS Writers group

Cti-Group Policy Creator Owners group

Cti-Guest user

Cti-John Smith user

Cti-Kerberos user

Cti-RAS and IAS Servers group

Cti-Read-only Domain Controllers group

Cti-Schema Admins group

Cti-Taher Ebar user



## 2. Configuring SSO on the FortiGate

Go to **User & Device > Authentication > Single Sign-On** and create a new SSO server.

In the **Type** field, select **Fortinet Single-Sign-On Agent**.

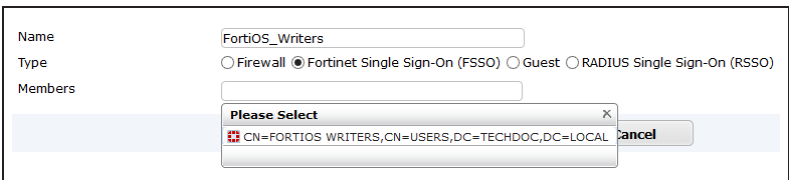
When selecting the **Users/Groups** field, the SSO user groups initially polled by the FortiAuthenticator from the Domain Controller, shows up in the FortiGate.

In this example, only the "FortiOS writers" group shows up because of the **FortiGate Filtering** configured in the previous step.

|                         |   |   |
|-------------------------|---|---|
| Name                    | FAC-techdoc.local                       |   |
| Primary Agent IP/Name   | 10.10.20.10                             | Password <input type="password" value="....."/> |
| Secondary Agent IP/Name |   | Password <input type="password" value="....."/> |
| LDAP Server             | Click to set...                         |   |
| Users/Groups            | CN=FORTIOS WRITERS,CN=USERS,DC=TECHD... |   |

### 3. Creating a user group on the FortiGate

Go to **User & Device > User > User Groups** and create a new user group. Under **Members**, select the user group to be monitored. In this example only "FortiOS Writers" shows up because of the **FortiGate Filtering** configured earlier.



Name: FortiOS\_Writers

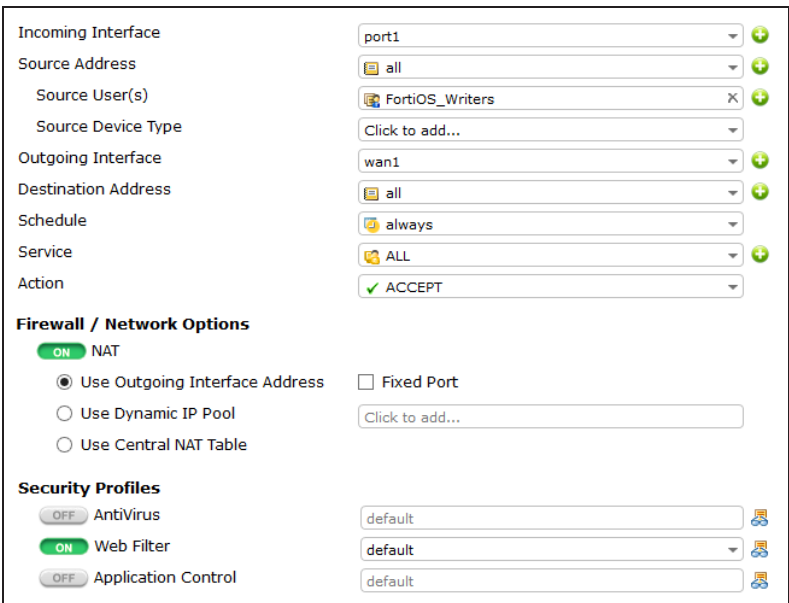
Type: ☐ Firewall ☒ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: **Please Select** (dialog box showing 'CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL' selected)

### 4. Adding a policy in the FortiGate

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing "FortiOS\_writers" to navigate the Internet with appropriate security profiles.

The default **Web Filter** security profile is used in this example.



Incoming Interface: port1

Source Address: all

Source User(s): FortiOS\_Writers

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

☒ ON NAT

☒ Use Outgoing Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

**Security Profiles**

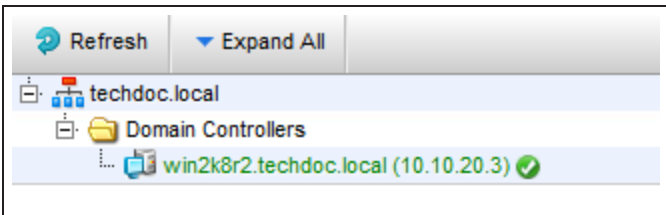
☐ OFF AntiVirus

☒ ON Web Filter

☐ OFF Application Control

### 5. Results from the FortiAuthenticator

Go to **Monitor > SSO > Domains** to verify monitored domains. In this Example "techdoc.local" is monitored by the FortiAuthenticator.



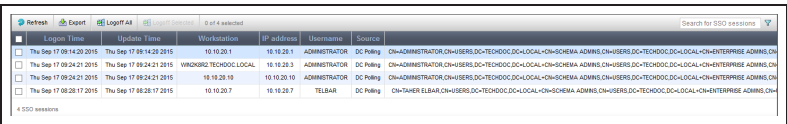
Refresh Expand All

techdoc.local

Domain Controllers

win2k8r2.techdoc.local (10.10.20.3) ✓


Have users log on to the domain, and go to **Monitor > SSO > SSO Sessions** and verify SSO sessions.



A screenshot of the 'SSO Sessions' table in a web application. The table has columns: Logon Time, Update Time, Workstation, IP address, Username, and Source. It shows several rows of session data, including logon times, update times, workstation names, IP addresses, usernames, and source information.

| Logon Time               | Update Time              | Workstation | IP address  | Username      | Source    |
|--------------------------|--------------------------|-------------|-------------|---------------|-----------|
| The Sep 17 09:14:20 2015 | The Sep 17 09:14:20 2015 | 10.10.20.1  | 10.10.20.1  | ADMINISTRATOR | DC Policy |
| The Sep 17 09:14:20 2015 | The Sep 17 09:14:20 2015 | 10.10.20.3  | 10.10.20.3  | ADMINISTRATOR | DC Policy |
| The Sep 17 09:24:21 2015 | The Sep 17 09:24:21 2015 | 10.10.20.10 | 10.10.20.10 | ADMINISTRATOR | DC Policy |
| The Sep 17 09:24:21 2015 | The Sep 17 09:24:21 2015 | 10.10.20.7  | 10.10.20.7  | ADMINISTRATOR | DC Policy |

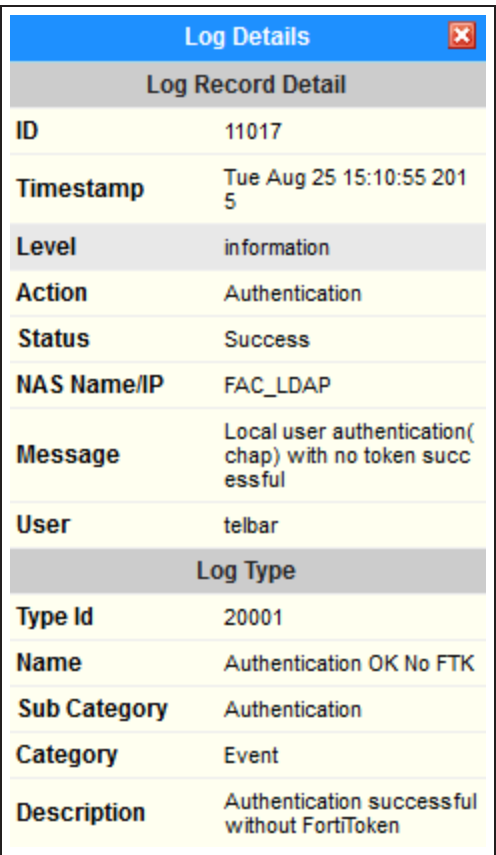
Go to **Logging > Log Access > Logs** to verify logs.



A screenshot of the 'Log Access' table in a web application. The table has columns: ID, Timestamp, Level, Category, Sub Category, Type Id, Action, Status, NAS Name/IP, and Message. It shows several rows of log data, including IDs, timestamps, levels, categories, sub categories, type IDs, actions, statuses, NAS names/IPs, and messages.

| ID    | Timestamp                | Level       | Category | Sub Category   | Type Id | Action         | Status  | NAS Name/IP | Message  |
|-------|--------------------------|-------------|----------|----------------|---------|----------------|---------|-------------|--|
| 11025 | The Sep 17 09:10:10 2015 | Information | Event    | Authentication | 20001   | Authentication | Success | FAC_LDAP    | Local user authentication(chap) with no token successful |
| 11024 | The Sep 17 09:10:10 2015 | Information | Event    | Authentication | 20001   | Authentication | Success | FAC_LDAP    | Local user authentication(chap) with no token successful |
| 11023 | The Sep 17 09:10:10 2015 | Information | Event    | Authentication | 20001   | Authentication | Success | FAC_LDAP    | Local user authentication(chap) with no token successful |

Select an entry for details.

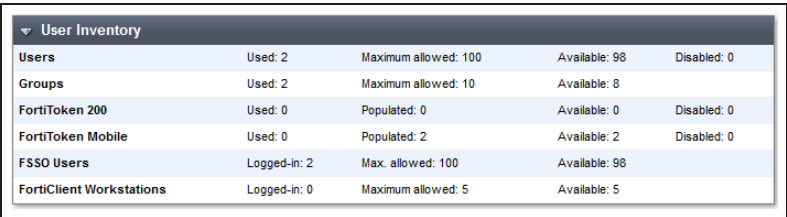


A screenshot of the 'Log Details' dialog box in a web application. The dialog has a title bar 'Log Details' and a close button. It contains a 'Log Record Detail' section with fields: ID (11017), Timestamp (Tue Aug 25 15:10:55 2015), Level (information), Action (Authentication), Status (Success), NAS Name/IP (FAC\_LDAP), Message (Local user authentication(chap) with no token successful), and User (telbar). Below this is a 'Log Type' section with fields: Type Id (20001), Name (Authentication OK No FTK), Sub Category (Authentication), Category (Event), and Description (Authentication successful without FortiToken).

| Log Record Detail |  |
|-------------------|--|
| ID                | 11017  |
| Timestamp         | Tue Aug 25 15:10:55 2015                                 |
| Level             | information  |
| Action            | Authentication   |
| Status            | Success  |
| NAS Name/IP       | FAC_LDAP   |
| Message           | Local user authentication(chap) with no token successful |
| User              | telbar   |

| Log Type     |  |
|--------------|--|
| Type Id      | 20001  |
| Name         | Authentication OK No FTK                     |
| Sub Category | Authentication                               |
| Category     | Event  |
| Description  | Authentication successful without FortiToken |

You can also verify results in the **User inventory** widget under **System > Dashboard > Status**.



A screenshot of the 'User Inventory' table in a web application. The table has columns: Users, Groups, FortiToken 200, FortiToken Mobile, FSSO Users, and FortiClient Workstations. It shows several rows of user inventory data, including user counts, group counts, FortiToken counts, FortiToken Mobile counts, FSSO counts, and FortiClient counts.

| Users                | Groups              | FortiToken 200 | FortiToken Mobile | FSSO Users        | FortiClient Workstations |
|----------------------|---------------------|----------------|-------------------|-------------------|--------------------------|
| Used: 2              | Used: 2             | Used: 0        | Used: 0           | Logged-in: 2      | Logged-in: 0             |
| Maximum allowed: 100 | Maximum allowed: 10 | Populated: 0   | Populated: 2      | Max. allowed: 100 | Maximum allowed: 5       |
| Available: 98        | Available: 8        | Available: 0   | Available: 2      | Available: 98     | Available: 5             |
| Disabled: 0          | Disabled: 0         | Disabled: 0    | Disabled: 0       |                   |                          |

## 6. Results from the FortiGate

Upon successful authentication, go to **User & Device > Monitor > Firewall** and verify FSSO Logons.

| Refresh  de-authenticate |                 |                                |              |                  |          |
|--------------------------|-----------------|--------------------------------|--------------|------------------|----------|
| ▼ User Name              | ▼ User Group    | ▼ Duration                     | ▼ IP Address | ▼ Traffic Volume | ▼ Method |
| ADMINISTRATOR            | FortiOS_Writers | 0 day(s) 0 hour(s) 7 minute(s) | 10.10.20.1   | N/A              | FSSO     |
| ADMINISTRATOR            | FortiOS_Writers | 0 day(s) 0 hour(s) 7 minute(s) | 10.10.20.3   | 1.61 KB          | FSSO     |
| TELBAR                   | FortiOS_Writers | 0 day(s) 0 hour(s) 7 minute(s) | 10.10.20.7   | N/A              | FSSO     |
| ADMINISTRATOR            | FortiOS_Writers | 0 day(s) 0 hour(s) 7 minute(s) | 10.10.20.10  | 2.36 KB          | FSSO     |

Have authenticated user navigate the Internet. Security profiles will be applied accordingly.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify the log.

| #  | Date/Time | Source                     | Destination                              | Application Name | Sent / Received    | Action | User          |
|----|-----------|----------------------------|--|------------------|--------------------|--------|---------------|
| 1  | 06:35:54  | TELBAR (10.10.20.7)        | 68.67.153.53                             | HTTP             | 529 B / 1.09 KB    | close  | TELBAR        |
| 2  | 06:35:54  | TELBAR (10.10.20.7)        | 68.67.153.53                             | HTTP             | 4.90 KB / 16.25 KB | close  | TELBAR        |
| 3  | 06:35:54  | TELBAR (10.10.20.7)        | 68.67.153.53                             | HTTPS            | 1.64 KB / 3.76 KB  | close  | TELBAR        |
| 4  | 06:35:53  | TELBAR (10.10.20.7)        | 68.67.153.40                             | HTTP             | 942 B / 1.18 KB    | close  | TELBAR        |
| 5  | 06:35:50  | TELBAR (10.10.20.7)        | 207.46.15.282                            | HTTPS            | 1.95 KB / 6.64 KB  | close  | TELBAR        |
| 6  | 06:35:50  | TELBAR (10.10.20.7)        | 234.1.94                                 | HTTP             | 635 B / 870 B      | close  | TELBAR        |
| 7  | 06:35:48  | TELBAR (10.10.20.7)        | 131.253.61.88 (login.live.com)           | HTTPS            | 1.52 KB / 6.10 KB  | close  | TELBAR        |
| 8  | 06:35:48  | TELBAR (10.10.20.7)        | 64.74.232.42                             | HTTP             | 989 B / 549 B      | close  | TELBAR        |
| 9  | 06:35:48  | TELBAR (10.10.20.7)        | 64.74.232.42                             | HTTP             | 714 B / 476 B      | close  | TELBAR        |
| 10 | 06:35:46  | ADMINISTRATOR (10.10.20.3) | 8.8.8.8 (google-public-dns-a.google.com) | DNS              | 81 B / 81 B        | accept | ADMINISTRATOR |

Select an entry for details.

|                     |                                      |                       |                     |
|---------------------|--------------------------------------|-----------------------|---------------------|
| #                   | 1                                    | Action                | close               |
| Date/Time           | 06:35:54                             | Destination           | 68.67.153.53        |
| Destination Country | United States                        | Destination Interface | wan1                |
| Destination Port    | 80                                   | Duration              | 17                  |
| Group               | FortiOS_Writers                      | Level                 |                     |
| Log ID              | 13                                   | Policy ID             | 9                   |
| Policy UUID         | 1014caf4-3541-51e5-8733-9d89435a30ff | Protocol              | tcp                 |
| Protocol Number     | 6                                    | Received Bytes        | 1092                |
| Received Packets    | 4                                    | Sent Bytes            | 929                 |
| Sent Packets        | 6                                    | Sequence Number       | 4763305             |
| Service             | HTTP                                 | Source                | TELBAR (10.10.20.7) |
| Source Country      | Reserved                             | Source Interface      | port1               |
| Source Port         | 58952                                | Src NAT IP            | 172.20.120.22       |
| Src NAT Port        | 58952                                | Sub Type              | forward             |
| Timestamp           | 9/17/2015, 6:35:54 AM                | Tran Display          | snat                |
| User                | TELBAR                               | Virtual Domain        | root                |

# Hub-and-spoke VPN using quick mode selectors

In this expert cookbook article and an included example recipe, we will explore a scalable approach to setting up a large number of spoke VPNs by using quick mode selector source definitions on the spoke FortiGates and the dialup VPN configurations on the hub FortiGates.

We will also explore how redundant spoke VPN tunnels can be configured in order to offer maximum redundancy for environments with critical availability requirements. We will be authenticating the VPN tunnels using X-Auth in order to ensure separate credentials for each spoke.

This recipe is based on FortiOS firmware version 5.2, so some of the steps shown may not be the same as with other versions of the firmware.

The sample topology for this advanced cookbook article follows:

This topology consists of 2 hub networks and 2 spoke networks, using private IP ranges, separated by a simulated Internet, with 100.64.0.0/16 representing the Internet. Each FortiGate also has a loopback interface that is routable across the VPN.

The diagram topology shows the VPN tunnels along with their redundant links:

- The **red** dotted line showing the VPN tunnel connection between the primary and backup data centers; in this case, our two hubs.
- The **blue** dotted line showing the VPN tunnel connection between the primary datacenter and the branch offices; the spokes in the scenario.
- The **orange** dotted line shows the VPN tunnel connection between the backup datacenter and the branch offices.

While the topology shown in the diagram can be built using individual static tunnels between each site, this would not scale well if addition spokes grow to a significant number. There would also be limited support for dynamically addressed sites. This strategy put forth by this article offers a solution to these issues by using a single phase 1 dialup definition on the hub FortiGates with additional spoke tunnels being added, without any changes to the hubs beyond that of adding additional user accounts for each additional spoke.

Spoke authentication is maintained by with X-Auth, which keeps the authentication of the individual tunnels separate in such a way that the use of a Pre-Shared Key alone is insufficient to authenticate a tunnel. A Public Key Infrastructure can also be used, provided that separate key-pairs are used for each VPN tunnel to maintain the segregation of the spokes.

The key points of this design are:

- Each hub FortiGate is configured with a dialup interface-mode Phase1 using X-Auth.

- Each spoke has its own user account on the hub FortiGates. In this example, local accounts are used on each hub, but a RADIUS or LDAP authentication server could be used on the back end, eliminating the need to managed the accounts on the FortiGates.
- Spoke FortiGates are configured to propagate their local subnets using quick mode selectors (specifically, a source object).
- When a new spoke tunnel is connected, the hub FortiGate validates the shared secret along with the X-Auth credentials provided by the spoke FortiGate.
- Spokes FortiGates can have dynamically assigned IP addresses such as those given out by DSL or cable ISPs.
- The hub FortiGates each insert a reverse route pointing to newly established tunnel interfaces, for any of the subnets provided by the spoke FortiGate's source quick mode selectors.
- Each spoke FortiGate uses configured static routes to direct traffic that needs to go to the datacenter(s) through the VPN tunnels destined for the hubs. The static route to the backup hub is set to a higher priority number value, making it the less preferred route. There is also an option where you can send all of your traffic from the spokes through the VPN tunnel by default. This can be done by configuring the WAN interface to route all traffic through the public IP address of the hub FortiGate. This is what our example configuration is set to do.
- We need to aware of any potential points where asymmetrical routing could occur as it relates to traffic returning to the spokes (This is essentially the response to a request coming back through a different route than it took to get there). This can be a potential problem especially when communicating to hosts that are connected to both data centers and we happen to be redistributing spoke routes using a dynamic routing protocol with hub sites using OSI Layer 3 networking devices. In this case, we would ensure that the backup hub's redistributed routes are less preferred than the primary hub's routes. In all cases, it is important to have a clear view of the routing flows between each endpoint and to keep "diag debug flow" in our toolbox to diagnose those potential asymmetric routing issues. In our example, we would want to route traffic destined to resources in each respective hub directly to that hub, rather than have it cross the inter-datacenter VPN tunnel, and have default routing flow to the primary hub under normal circumstances.

## The Hub FortiGates

Let's look at the relevant configuration points of the hub FortiGates (These will be identical on each hub FortiGate:

While the GUI can be used for these steps, we are going to use the CLI to keep things simple and avoid potential confusion that may be caused by changes in the GUI's layout.

### Create the IPsec tunnel:

```
config vpn ipsec phase1-interface
edit "SPOKES"
set type dynamic
set interface "port1"
set mode aggressive
set peertype one
```

```

    set proposal aes256-sha256
    set xauthtype auto
    set authusrgrp "SPOKE-GRP"
    set peerid "SPOKES"
    set psksecret SuperSecretSpokeSecret
    next
end

config vpn ipsec phase2-interface
    edit "SPOKES-P2"
    set phase1name "SPOKES"
    set proposal aes256-sha256
    set keepalive enable
    next
end

```

### Create a user for each of the spokes:

```

config user local
    edit "SPOKE1"
    set type password
    set passwd Spoke1SuperSecret
    next
    edit "SPOKE2"
    set type password
    set passwd Spoke2SuperSecret
    next
end

```

### Create a user group and include the spoke members:

```

config user group
    edit "SPOKE-GRP"
    set member "SPOKE1" "SPOKE2"
    next
end

```

## Create the firewall policies

```
config firewall policy
  edit 1
    set srcintf "port2" "loop0"
    set dstintf "SPOKES"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
  edit 2
    set srcintf "SPOKES"
    set dstintf "port2" "loop0"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```

A few of the above configuration aspects require further explanation:

- **Aggressive mode:** We are using this mode in order to ensure that these dialup spokes are terminated on the right dialup phase1. If the hub unit has other dialup phase1 (for FortiClient VPN users, for instance), the hub would otherwise be unable to distinguish between each dialup phase1. A few of the above configuration aspects require further explanation:
- **X-Auth:** As previously stated, this allows us to authenticate each connecting spoke unit to a local group, which is defined in the above configuration as currently containing two user accounts (our example has two spokes). Provisioning additional spokes on the hub would simply involve adding additional user accounts.
- **Policies:** As usual, we must always configure policies in order for traffic to flow. IPsec Phase1 follows a special rule in which tunnels will not even attempt to come up unless they have at least one policy referring to them (this happens to be a good trick to know when you want to disable an IPsec VPN tunnel without deleting its configuration).

## The Spoke FortiGates

With the hub FortiGates configured and ready for incoming connections, the spoke FortiGates can be configured. Below is the steps for configuring SPOKE1. To configure additional spoke FortiGates change the unit specific information.



## Create the IPsec tunnel

```
config vpn ipsec phase1-interface
    edit "HUB-PRIMARY"
        set interface "port1"
        set mode aggressive
        set proposal aes256-sha256
        set localid "SPOKES"
        set xauthtype client
        set authusr "SPOKE1"
        set authpasswd Spoke1SuperSecret
        set mesh-selector-type subnet
        set remote-gw 100.64.10.2
        set psksecret SuperSecretSpokeSecret
    next
    edit "HUB-BACKUP"
        set interface "port1"
        set mode aggressive
        set proposal aes256-sha256
        set localid "SPOKES"
        set xauthtype client
        set authusr "SPOKE1"
        set authpasswd Spoke1SuperSecret
        set mesh-selector-type subnet
        set remote-gw 100.64.11.2
        set psksecret SuperSecretSpokeSecret
    next
end

config vpn ipsec phase2-interface
    edit "PRIMARY-P2"
        set phase1name "HUB-PRIMARY"
        set proposal aes256-sha256
        set keepalive enable
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN_SUBNETS"
        set dst-name "all"
    next
    edit "BACKUP-P2"
        set phase1name "HUB-BACKUP"
        set proposal aes256-sha256
        set keepalive enable
        set src-addr-type name
        set dst-addr-type name
```

```
    set src-name "VPN_SUBNETS"
    set dst-name "all"
  next
end
```

## Creating addresses for the subnets

```
config firewall address
  edit "NET_192.168.12.0/24"
  set subnet 192.168.12.0 255.255.255.0
  next
  edit "NET_100.64.254.12/32"
  set subnet 100.64.12.254 255.255.255.255
  next
end
```

## Creating an address group for the subnets

```
config firewall addrgrp
  edit "VPN_SUBNETS"
  set member "NET_100.64.254.12/32" "NET_192.168.12.0/24"
  next
end
```

## Configuring static routes

Use edit 0 to create a route with the next unused number.

```
config router static
  edit 0
  set dst 100.64.11.2 255.255.255.255
  set device "port1"
  next
  edit 0
  set dst 100.64.10.2 255.255.255.255
  set device "port1"
  next
  edit 0
  set device "HUB-PRIMARY"
  next
  edit 0
  set device "HUB-BACKUP"
  set priority 20
  next
end
```

## Configuring the firewall policies

Use edit 0 to create a policy with the next unused number.

```
config firewall policy
  edit 0
    set srcintf "port2" "loop0"
    set dstintf "HUB-PRIMARY"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
  edit 0
    set srcintf "HUB-PRIMARY"
    set dstintf "port2" "loop0"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
  edit 0
    set srcintf "port2" "loop0"
    set dstintf "HUB-BACKUP"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
  edit 0
    set srcintf "HUB-BACKUP"
    set dstintf "port2" "loop0"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```

Each spoke configuration calls for similar Phase1 parameters, but differs for the rest of the configuration in a few keys areas:

- **Aggressive mode:** As the hub is validating the inbound ID, we have configured our peer ID to the matching string "SPOKES".
- **X-Auth:** Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.
- **Phase 2 quick mode selectors:** As the title of this recipe suggests, this is where the spoke provisioning routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the "set mesh-selector-type subnet" command must be configured to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group.
- **Routing:** As previously expressed, we have configured our default routing to flow through the primary hub ([blue links](#)) and failover routing to the backup hub ([orange links](#), using route priority adjustment). Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

## Where the spoke configurations will be different

As explained earlier, the spoke FortiGate configurations will be slightly different on each individual spoke. The settings will be similar on all of the spoke with the following exceptions:

- **X-Auth:** Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.

```
config vpn ipsec phase1-interface
edit "HUB-PRIMARY"
    set authusr (The account will be the one associated with the specific spoke)
    set authpasswd (The password will be the one associated with the specific spoke)
next
edit "HUB-BACKUP"
    set authusr (The account will be the one associated with the specific spoke)
    set authpasswd (The password will be the one associated with the specific spoke)
next
end
```

- **Phase 2 quick mode selectors:** This is where the spoke routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the following setting must be used to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group:

```
config vpn ipsec phase1-interface
edit <name>
    set mesh-selector-type subnet
end
end
```

- **Routing:** This won't necessarily be different between the different spoke FortiGates, but as previously mentioned, in this example recipe we have configured our default routing to flow through the primary hub and failover routing to the backup hub. Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

## Results

And this concludes our VPN configuration! But this recipe would not be complete without a very important verification step. Let's look at the routing table on the hub:

```
HUB # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S*      0.0.0.0/0 [10/0] via 192.168.56.2, port1
S       100.64.254.12/32 [15/0] is directly connected, HUB_0S
100.64.254.13/24 [15/0] is directly connected, HUB_1
C       192.168.11.0/24 is directly connected, port2
S       192.168.12.0/24 [15/0] is directly connected, HUB_0S
192.168.13.0/24 [15/0] is directly connected, HUB_1
C       192.168.56.0/24 is directly connected, port1
```

As can be seen above, our spoke subnets have been automatically injected into the hub's routing tables. A closer look at the VPN details of one spoke confirms that the hub received the negotiated subnets during quick mode negotiation and inserted distinct SAs for each SA.

```
FGT1 # get vpn ipsec tunnel details
gateway
name: 'HUB_0'
type: route-based
local-gateway: 192.168.56.11:0 (static)
remote-gateway: 192.168.56.12:0 (dynamic)
mode: ike-v1
interface: 'port1' (2)
rx packets: 56 bytes: 8736 errors: 0
tx packets: 41 bytes: 3444 errors: 0
dpd: enabled/negotiated idle: 5000ms retry: 3 count: 0
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:192.168.12.0-192.168.12.255:0
-----OUTPUT TRUNCATED-----
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:100.64.254.12-100.64.254.12:0
```

-----OUTPUT TRUNCATED-----

If you require communication between the spokes, this can be routed through the hub FortiGates. The only change to the example recipe's configuration is an addition policy on each of the hub FortiGates which defines the both the Incoming Interface and the Outgoing Interface as the VPN Dialup Interface (in this example, SPOKES)

On the Spoke FortiGates, once the poke tunnels have been established, you can see the default route to the primary datacenter and the alternate though less preferred route to the backup datacenter by running the

```
command get router info routing-table all
FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-PRIMARY [10/0] is
directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0
C 192.168.12.0/24 is directly connected, port2
```

We can test the failover function by shutting down the port1 interface on the primary hub. This will bring down the VPN between the primary hub and the spokes. Once the DPD detects the fault, traffic switches over to the backup hub as shown here:

```
FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0C 192.168.12.0/24 is directly
connected, port2
```

## Final notes

- The technique shown here does not involve dynamic routing so this configuration and its very straight forward template can be easily used to scale up the topology to include thousands of spoke sites.
- To make it even easier, this configuration can be entirely built and automated with FortiManager, which has support for provisioning hub-and-spoke dialup topologies.

# Glossary

- BGP:** Border Gateway Protocol is primarily used to connect the networks of large organizations that have two or more ISP connections, or between other autonomous systems. If used in such a situation, a FortiGate can use BGP for routing.
- BYOD:** Bring Your Own Device (also called device management) is the practice of allowing network users to access an organization's (usually wireless) network with their own computers, smart phones, tablets and other devices. BYOD has a major impact on networks with large and diverse user bases, such as educational institutions, but also affects large and small business networks.
- CA:** A certificate authority (CA) is an entity that issues digital certificates, which are used to establish secure connections over a network, typically the Internet. The CA acts as a trusted third-party by verifying the identity of a certificate's owner: for example, the certificate found when you go to <https://www.facebook.com> is verified as belonging to Facebook.
- Certificates:** In networking, certificates (including public key certificates, digital certificates, and identity certificates) provide digital signatures for websites or other electronic communication and allow you to verify whether a digital identity is legitimate.. A FortiGate can use certificates for many things, including SSL inspection and user authentication.
- CLI:** The Command Line Interface is a text-based interface used to configure a FortiGate unit. Most steps in the FortiGate Cookbook use the Graphical User Interface (see GUI), but some configuration options are only available using the CLI.
- DHCP:** Dynamic Host Configuration Protocol is a networking protocol that allows devices to request network parameters, such as IP addresses, automatically from a DHCP server, reducing the need to assign these settings manually. A FortiGate can function as a DHCP server for your network and can also receive its own network parameters from an external DHCP server.
- Dial-up/dynamic VPN:** A dial-up VPN, also called a dynamic VPN, is a type of IPsec VPN where one of the endpoints has a dynamic IP address.
- DMZ:** A Demilitarized Zone is an interface on a FortiGate unit that provides external users with secure access to a protected subnet on the internal network without giving them access to other parts of the network. This is most commonly done for subnets containing web servers, which must be accessible from the Internet. The DMZ interface will only allow traffic that has been explicitly allowed in the FortiGate's configuration. FortiGate models that do not have a DMZ interface can use other interfaces for this purpose.
- DNS:** Domain Name System is used by devices connecting to the Internet to locate websites by mapping a domain name to a website's IP address. For example, a DNS server maps the domain name [www.fortinet.com](http://www.fortinet.com) to the IP address 66.171.121.34. Your FortiGate unit controls which DNS servers the network uses. A FortiGate can also function as a DNS server.
- DSR:** In a typical load balancing scenario, server responses to client requests are routed through a load balancer on their way back to the client. The load balancer examines the headers of each response and can insert a cookie before sending the server response on to the client. In a Direct Server Return (DSR) configuration, the server receiving a client request responds directly to the client IP, bypassing the load balancer. Because the load balancer only processes incoming requests, load balancing performance is dramatically improved when using

DSR in high bandwidth applications. In such applications, it is not necessary for the load balancer to receive and examine the server's responses. So the client makes a request and the server simply streams a large amount of data to the client.

### **Dynamic IP address:**

A dynamic IP address is one that can change without the device's user having to do anything. Dynamic IP addresses allow networks to control the IP addresses of devices that connect to them. This allows you to connect portable devices to different networks without needing to manually change their IP addresses.

Dynamic IP addresses are set by network protocols, most often DHCP.

### **ECMP:**

Equal Cost Multipath Routing allows next-hop packet forwarding to a single destination to occur over multiple best paths that have the same value in routing metric calculations. ECMP is used by a FortiGate for a variety of purposes, including load balancing.

### **Explicit Proxy:**

Explicit proxy is a type of configuration where all clients are configured to allow requests to go through a proxy server, which is a server used as an intermediary for requests from clients seeking resources from other servers. When a FortiGate uses explicit proxy, the clients sending traffic are given the IP address and port number of the proxy server.

### **FGCP:**

FortiGate Clustering Protocol is used for high availability (HA).

### **FortiAP:**

A FortiAP unit is a wireless Access Point that can be managed by a FortiGate. Most FortiAP functions can also be accomplished using a FortiWiFi unit.

### **FortiClient:**

The FortiClient software provides a variety of features, including antivirus, web filtering, firewall, and parental controls, to individual computers and mobile devices. It can also be used to connect to a FortiGate using either an SSL or IPsec VPN.

FortiClient is available for Windows, Mac OSX, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more.

FortiClient can be downloaded at [www.forticlient.com](http://www.forticlient.com).

### **FortiOS:**

FortiOS is the operating system used by FortiGate and FortiWiFi units. It is also referred to as firmware.

### **FTP:**

File Transfer Protocol is a standard protocol used to transfer computer files from one host to another host over a computer network, usually the Internet, using FTP client and server applications.

### **Gateway:**

A gateway is the IP address that traffic is sent to if it needs to reach resources that are not located on the local subnet. In most FortiGate configurations, a default route using a gateway provided by an Internet service provider must be set to allow Internet traffic.

### **GUI:**

The Graphical User Interface, also known as the web-based manager, is a graphics-based interface used to configure a FortiGate unit and is an alternative to using the Command Line Interface (see CLI). You can connect to the GUI using either a web browser or FortiExplorer. Most steps in the FortiGate Cookbook use the GUI.

### **HTTP:**

Hypertext Transfer Protocol is a protocol used for unencrypted communication over computer networks, including the Internet, where it is used to access websites. FortiGate units handle more HTTP traffic than any other protocol.



|                      |   |
|----------------------|---|
| <b>HTTPS:</b>        | Hypertext Transfer Protocol Secure is a protocol that secures HTTP communications using the Secure Sockets Layer (SSL) protocol. HTTPS is the most commonly used secure communication protocol on the Internet.   |
| <b>Interfaces:</b>   | Interfaces are the points at which communication between two different environments takes place. These points can be physical, like the Ethernet ports on a FortiGate, or logical, like a VPN portal.   |
| <b>IP address:</b>   | An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. FortiGate units can use IP addresses to filter traffic and determine whether to allow or deny traffic. Both IP version 4 and IP version 6 (see IPv4 and IPv6) are supported by your FortiGate.   |
| <b>IPsec:</b>        | Internet Protocol Security is used to for securing IP communications by authenticating and encrypting each packet of a session. A FortiGate primarily uses this protocol to secure virtual private networks (see VPN).  |
| <b>IPv4:</b>         | Internet Protocol version 4 is the fourth version of the Internet Protocol (IP), the main protocol used for communication over the Internet. IPv4 addresses are 32-bit and can be represented in notation by 4 octets of decimal digits, separated by a period: for example, 172.16.254.1.  |
| <b>IPv6:</b>         | Internet Protocol version 6 is the sixth version of the Internet Protocol (IP), the main protocol used for communication over the Internet (IPv5 never became an official protocol). IPv6 was created in response to the depletion of available IPv4 addresses. IPv6 addresses are 128-bit and can be represented in notation by 8 octets of hexadecimal digits, separated by a colon: for example, 2001:db8:0000:0000:0000:0000:0000:0000. IPv6 addresses can be shortened if all the octets are 0000; for example, the previous address can also be written as 2001:db8:: |
| <b>LAN/internal:</b> | The LAN/internal interface is an interface that some FortiGate models have by default. This interface contains a number of physical ports that are all treated as a single interface by the FortiGate unit. This allows you to configure access for the entire Local Area Network at the same time, rather than configuring each port individually.   |
| <b>LDAP:</b>         | Lightweight Directory Access Protocol is a protocol used for accessing and maintaining distributed directory information services over a network. LDAP servers are commonly used with a FortiGate for user authentication.  |
| <b>MAC address:</b>  | A Media Access Control address is a unique identifier assigned to a network interface used for network communication. A MAC address is assigned to a device by the manufacturer and so this address, unlike an IP address, is not normally changed. MAC addresses are represented in notation by six groups of two hexadecimal digits, separated by hyphens or colons: for example, 01:23:45:67:89:ab. Your FortiGate can identify network devices using MAC addresses.   |
| <b>Multicast:</b>    | Multicast is a method of group communication where information is addressed to a group of destinations simultaneously. A FortiGate can use multicast traffic to allow communication between network devices.  |
| <b>NAT:</b>          | Network Address Translation is a process used to modify, or translate, either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the internet. FortiGate also supports many other uses for NAT.  |
| <b>Netmask</b>       | A netmask, or subnet mask, is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.   |

|                          |  |
|--------------------------|--|
| <b>Packet:</b>           | A packet is a unit of data that is transmitted between communicating devices. A packet contains both the message being sent and control information, such as the source address (the IP address of the device that sent the packet) and the destination address (the IP address of the device the packet is being sent to).  |
| <b>Ping:</b>             | Ping is a utility used to test whether devices are connected over a IP network and to measure how long it takes for a reply to be received after the message is sent, using a protocol called Internet Control Message Protocol (ICMP). If ICMP is enabled on the destination interface, you can ping the IP address of a FortiGate interface to test connectivity between your computer and the FortiGate. You can also use the CLI command <code>execute ping</code> to test connectivity between your FortiGate and both internal and external devices. |
| <b>Ports:</b>            | See Interfaces and Port Numbers.   |
| <b>Port numbers:</b>     | Port numbers are communication endpoints used to allow network communication. Different ports are used for different application-specific or process-specific purposes; for example, HTTP protocol commonly uses port 80.  |
| <b>Pre-shared key:</b>   | <p>In cryptography, a pre-shared key is a character string (like a password) known by two parties, and used by those parties to identify each other. Pre-shared keys are commonly used for granting access to IPsec VPNs and WiFi networks.</p> <p>Pre-shared keys are different from regular passwords because they are not normally associated with a specific individual's credentials.</p>   |
| <b>RADIUS:</b>           | Remote Authentication Dial In User Service is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. RADIUS servers are commonly used with a FortiGate for user authentication, including single-sign on.   |
| <b>RTSP:</b>             | <p>The Real Time Streaming Protocol is a media control protocol that is used for controlling streaming audio and video streams. RTSP has a wide range of uses and is often leveraged by other media-related services such as SIP. It most commonly uses TCP and UDP port 554 but additional ports are used by the actual media controlled by RTSP.</p> <p>FortiOS includes an RSTP session helper that opens the ports used by individual RTSP-controlled streams. FortiRecorder and FortiCamera use RTSP for video streaming.</p>                         |
| <b>SCTP:</b>             | The Stream Control Transmission Protocol is a transport layer protocol (protocol number 132) used most often for sending telephone signalling messages over carrier IP networks.   |
| <b>Session:</b>          | A session is the dialogue between two or more communicating devices that include all messages that pass between the devices; for example, a session is created when a user browses to a specific website on the Internet for all communication between the user's computer and the web server that hosts the site. Sessions are tracked by a FortiGate unit in order to create logs about the network traffic.   |
| <b>SIP:</b>              | Session Initiation Protocol is used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol networks. FortiGate units use this protocol for voice over IP (see VoIP).   |
| <b>Site-to-site VPN:</b> | <p>A site-to-site VPN allows two networks that are each behind a VPN gateway (for example, a FortiGate unit), to establish secure connections with each other over a public network, typically the Internet.</p> <p>Site-to-site VPNs most often use IPsec and can be established between two FortiGates, or between a FortiGate and any other IPsec VPN gateway, such as a Cisco ASA or Microsoft Azure.</p>  |

|                                 |   |
|---------------------------------|---|
| <b>SLAAC:</b>                   | Stateless Address Autoconfiguration is a feature of IPv6 that allows devices on an IPv6 network to automatically get IPv6 addresses. SLAAC is similar to DHCP except that DHCP requires you to run and configure a DHCP server. SLAAC is built into IPv6 and requires only minor additional configuration. SLAAC is defined by <a href="#">RFC 2462</a> .   |
| <b>SNMP:</b>                    | Simple Network Management Protocol is a protocol that monitors hardware on your network. A FortiGate can use SNMP to monitor events such as high CPU usage, VPN tunnels going down, or hardware becoming disconnected.  |
| <b>SSH:</b>                     | Secure Shell is a protocol used for secure network services between two devices, including remote command-line access. SSH can be used to access a FortiGate's command line interface (CLI).  |
| <b>SSID:</b>                    | A Service Set Identifier is the name that a wireless access point broadcasts to wireless users. Wireless users select this name to join a wireless network.   |
| <b>SSL:</b>                     | Secure Sockets Layer is a protocol for encrypting information that is transmitted over a network, including the Internet. SSL can be used for secure communications to a FortiGate, as well as for encrypting Internet traffic (see HTTPS) and for allowing remote users to access a network using SSL virtual private network (see VPN).   |
| <b>SSL inspection:</b>          | Secure Sockets Layer inspection is used by your FortiGate to scan traffic or communication sessions that use SSL for encryption, including HTTPS protocol.  |
| <b>SSO:</b>                     | Single Sign-On is a feature that allows a user to login just once and remembers the credentials to re-use them automatically if additional authentication is required. A FortiGate supports both Fortinet single sign-on (FSSO) and single sign-on using a RADIUS server (RSSO).  |
| <b>Static IP address:</b>       | Static IP addresses require user intervention to change. Normally a device that always has a wired connection to an Ethernet network has a static IP address.   |
| <b>Static route:</b>            | A static route is a manually-configured routing entry that is fixed and does not change if the network is changed or reconfigured.  |
| <b>Subnet:</b>                  | A subnetwork, or subnet, is a segment of the network that is separated physically by routing network devices and/or logically by the difference in addressing of the nodes of the subnet from other subnets. Dividing the network into subnets helps performance by isolating traffic from segments of the network where it doesn't need to go, and it aids in security by isolating access. The addressing scope of a subnet is defined by its IP address and subnet mask and its connection to other networks is achieved by the use of gateways. |
| <b>Subnet Mask:</b>             | A subnet mask is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.  |
| <b>traceroute</b>               | <code>traceroute</code> is a diagnostic tool used to display the route of packets across an IP network and measure transit delays. <code>traceroute</code> can be useful to troubleshoot a connection and determine where an error is occurring.  |
| <b>Transport layer protocol</b> | A transport layer protocol provides end-to-end communication on top of the network layer (IP) layer for IP networks. Using a FortiGate, you can create security policies that control the following transport layer protocols: TCP (protocol number 6), UDP (protocol number 17), ICMP (protocol number 1), and SCTP (protocol number 132).   |

|                   |  |
|-------------------|--|
| <b>URL:</b>       | <p>A Uniform Resource Locator is a text string that refers to a network resource. The most common use for URLs is on the Internet, where they are also known as web addresses.</p> <p>URLs are used by a FortiGate to locate websites on the Internet and can also be used in web filtering to block specific sites from being accessed.</p> |
| <b>VDOM:</b>      | Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.  |
| <b>VLAN:</b>      | Virtual Local Area Networks are used to logically divide a single local area network (LAN) into different parts that function independently. A FortiGate uses VLANs to provide different levels of access to users connecting to the same LAN.   |
| <b>VoIP:</b>      | Voice over Internet Protocol is a protocol that is used to allow voice communications and multimedia sessions over Internet Protocol sessions, including the Internet. VoIP protocol is used by a FortiGate when traffic needs to reach a connected VoIP phone or FortiVoice unit.   |
| <b>VPN:</b>       | A Virtual Private Network is a private network that acts as a virtual tunnel across a public network, typically the Internet, and allows remote users to access resources on a private network. There are two main types of VPNs that can be configured using a FortiGate unit: IPsec VPN (see IPsec) and SSL VPN (see SSL).                 |
| <b>WAN/WAN 1:</b> | The WAN or WAN1 port on your FortiGate unit is the interface that is most commonly used to connect the FortiGate to a Wide Area Network, typically the Internet. Some FortiGate models have a WAN2 port, which is commonly used for redundant Internet connections.  |



The FortiGate Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

Written for FortiOS 5.2